Some Results on the Functional Decomposition of Polynomials

by
Mark William Giesbrecht
Department of Computer Science

A Thesis submitted in conformity with the requirements
for the Degree of Master's of Science in the
University of Toronto

Department of Computer Science
University of Toronto
Toronto, Ontario, Canada, M5S 1A4

Abstract

If g and h are functions over some field, we can consider their composition $f = g(h)$. The inverse problem is decomposition: given f, determine the existence of such functions g and h. In this thesis we consider functional decompositions of univariate and multivariate polynomials, and rational functions over a field F of characteristic p. In the polynomial case, "wild" behaviour occurs in both the mathematical and computational theory of the problem if p divides the degree of g. We consider the wild case in some depth, and deal with those polynomials whose decompositions are in some sense the "wildest": the additive polynomials. We determine the maximum number of decompositions and show some polynomial time algorithms for certain classes of polynomials with wild decompositions. For the rational function case we present a definition of the problem, a normalised version of the problem to which the general problem reduces, and an exponential time solution to the normal problem.

Acknowledgement.

I would like to thank my supervisor Dr. Joachim von zur Gathen for the long and fruitful hours he spent helping me with this thesis, and Dr. Rackoff for being my second reader. I would also like to thank my office mates and many others for their helpful suggestions and proof reading. Finally, I would like to thank NSERC for its scholarship support.

Table of Contents

Introduction.

A fundamental idea in computer science and mathematics is that of composition. One way to understand an object, whether it is abstract or concrete, is to understand how it combines with other objects of the same type. A converse problem to this also exists: Given an object, describe how it is made up as the composition of other objects. This is decomposition. We can introduce constraints on the decompositions we wish to examine. What happens when we cannot further break down the object under consideration given these constraints? We say it is indecomposable. A very natural question to look at is how an object under consideration breaks down into indecomposable pieces. And if we relax the constraints somewhat, do these indecomposable objects decompose once again? In mathematics, and especially algebra, decomposition is a central concept. Decomposing matrices, algebras and groups are all well explored areas. The factoring of polynomials is a fundamental example of the decomposition in the ring of polynomials under the usual operations of addition and multiplication. The computational aspects of factoring polynomials have been an extremely active area of research over the last two decades. But polynomials can also be composed functionally, and form a ring under addition and composition. What does factorisation in this ring look like? Although this question has been addressed mathematically for at least six decades, many unresolved questions still remain. Computationally the area is extremely new, having developed only over the last decade or so. Applications of polynomial decomposition within the areas of coding theory and cryptography exist (though will not be dealt with here), and the problem is of computational interest in its own right. Though some progress has been made in the (mathematically) well understood cases, the problem in general appears to be difficult. We will address ourselves to some of these difficulties.

If $f_m, f_{m-1}, \ldots, f_1$ are univariate polynomials over a field F of degrees $r_m, r_{m-1}, \ldots, r_1 \in \mathbb{N}$ respectively, their functional composition

$$f = f_m(f_{m-1}(\cdots(f_2(f_1))\cdots)) \in F[x]$$

has degree $n = r_m r_{m-1} \cdots r_1$, and can be computed in a straightforward manner. In this thesis we examine a converse problem. Namely, given f and $r_m, \ldots, r_1$, determine if there exist polynomials $f_m, \ldots, f_1 \in F[x]$ such that $\deg f_i = r_i$ for $1 \leq i \leq m$ and $f = f_m(f_{m-1}(\cdots(f_2(f_1))\cdots))$, and

if so, compute them. We call this the polynomial decomposition problem. When the problem is limited to decompositions into two composition factors of given degree, we call this the bidecomposition problem. A polynomial is considered to be indecomposable if there is no way to decompose it into non-trivial (degree at least two) composition factors. We also consider decompositions into indecomposable composition factors, which we call complete decompositions. Further questions arise when we consider decompositions over arbitrary algebraic extension fields of the ground field, or absolute decompositions. All these issues concerning decompositions have been dealt with mathematically since the seminal paper of Ritt[1922], which showed a very strong, "well behaved" structure for decompositions of polynomials over the complex numbers. Since then, the mathematical literature dealing with the problem has been extensive, though far from complete. The difficulty in the decomposition problem seems to be connected to the divisibility of the degrees by the characteristic p of the ground field. The "tame" case, where $p = 0$ or $p \nmid r_i$ for $1 < i \leq m$ is well understood. However, the "wild" case where $p|r_i$ for some $i > 1$ is still largely a mystery. It is this case in which we will be most interested.

For some special classes of polynomials, decompositions in the wild case are well understood. One such class is the "additive" polynomials. These are the polynomials where only exponents which are powers of the characteristic p of the field have non-zero coefficients. In some sense they are the "wildest" polynomials (see von zur Gathen[1988]). The theory of additive polynomials was introduced in Ore[1933b], and will be presented here in some detail. Kozen and Landau[1986] give an (exponential time) reduction of the general decomposition problem to univariate factorisation, and give a formulation of this problem in terms of the action of Galois groups. This turns out to be somewhat simpler for decompositions of separable, irreducible polynomials (over arbitrary fields) than in the general case. And for irreducible polynomials over finite fields they give a complete description of the decomposition structure.

Decompositions of multivariate polynomials have also been considered. Evyatar and Scott[1972] show a structure very similar to the univariate case. We consider decompositions of a multivariate polynomial f into a univariate polynomial g and a multivariate polynomial h. Completely analogous tame and wild cases exist, although even less is known about the wild case here than for univariate polynomials.

Computationally, polynomial decomposition has only been examined since 1976 by Barton and Zippel[1976,1985]. They give a general algorithm (for both the tame and wild cases) which requires a factoring subroutine and an exponential number of field operations in the degree of the input polynomial. Over arbitrary ("computable") fields, the decomposition problem is undecidable (see von zur Gathen[1988]). Kozen and Landau[1986] exhibit an algorithm for the bidecomposition problem in the tame case which requires only a polynomial number of field operations in the input degree. For multivariate polynomials there is a similar situation. Fast algorithms which compute decompositions do exist in the tame case (see Dickerson[1987] and von zur Gathen[1987]). And in the wild case we present an algorithm to perform multivariate decomposition (in an exponential number of field operations). Some special classes of the wild case have also been dealt with: Kozen and Landau[1986] give a decomposition algorithm for irreducible, separable polynomials which requires a quasi-polynomial number of field operations in the degree of the input, and for irreducible polynomials over finite fields, their algorithm requires only a polynomial number of field operations in the input degree.

This thesis is organised into six chapters. In chapter one we present a mathematical definition of the univariate decomposition problem and five different formulations of it. Each of these formulations has been used in the mathematical or computational literature, in various forms. Some were developed for special cases, and some fall immediately from the problem definition. We generalise these formulations and put them in a consistent language and context, showing their basic equivalence. We also define the multivariate problem in a similar manner, showing two basic, equivalent formulations.

In chapter two, we present the computational approaches to polynomial decomposition which have been developed for both the wild and tame cases. These algorithms will be stated in terms of the formulation of the decomposition problem used, as developed in chapter one. We show that for certain "nice" families of polynomials (polynomials for which an efficient algorithm for decomposition into two composition factors of given degree exists, and for which such decompositions are unique) the problem of decomposing a polynomial into an arbitrary number of factors of given degree is reducible to the bidecomposition problem. Using a structure theorem of Evyatar and Scott[1972], we also exhibit an algorithm for decomposing multivariate polynomials (in both the tame and wild cases) over any field supporting a fac-

toring algorithm.

In chapters three through five we introduce the additive polynomials, a class of polynomials with wild decompositions which are well understood. In chapter three we develop the theory of these polynomials with respect to the structure of their roots in their splitting fields. From this we garner quasi-polynomial lower bounds on the number of decompositions (both decompositions into two factors and complete decompositions) of "simple" additive polynomials. This shows that any algorithm which produces all decompositions of an arbitrary polynomial in the wild case cannot be expected to work in a polynomial number of field operations. In fact, we determine exactly the maximum number of decompositions of simple additive polynomials of a given degree.

In chapter four the theory of Ore[1933a], which describes non-commutative Euclidean rings, is developed for the additive polynomials. We extend this theory by further developing the relationship between different complete decompositions of a given polynomial. We also show a number of results concerning the uniqueness of decompositions. Combining this formal structure with the algebraic structure from chapter three, we show a quasi-polynomial upper bound on the number of possible complete decompositions of additive polynomials in general.

In chapter five we make use of the two previous chapters to develop algorithms for the decomposition of additive polynomials. We show that we can determine indecomposability in a polynomial number of field operations, and in fact can generate one complete decomposition. However, the only way method we know to find a decomposition into an arbitrary number of factors of given degrees is by finding all complete decompositions. Using the upper bound from chapter four, we get an algorithm requiring a quasi-polynomial number of field operations. Two large subclasses of the additive polynomials show more favourable results: the completely reducible additive polynomials and the similarity free additive polynomials. Decomposition algorithms requiring a polynomial number of field operations are shown in each case. We also show a quasi-polynomial time algorithm for the absolute decomposition of additive polynomials. This algorithm may well run in a polynomial number of field operations, subject to a conjectured (but unproven) upper bound on the degrees of splitting fields of additive polynomials. This conjecture follows immediately from a much stronger (and also unproven) conjecture of Ore[1933b].

In chapter six we define the rational function decomposition problem. We show a normalisation of this problem to a more a more uniquely defined form. We then show that the rational function decomposition problem is reducible to this normal rational function decomposition problem. Finally, we present an algorithm for solving the normal problem (in an exponential number of field operations in the input degree).

In summary the main original results of this thesis are:

(1) five equivalent formulations of the univariate decomposition problem and two formulations of the multivariate decomposition problem,

(2) a reduction from the general problem of finding decompositions into an arbitrary number of factors of given degree to the bidecomposition problem, for certain "nice" families of polynomials,

(3) an exponential time algorithm for decomposing multivariate polynomials (in both the tame and wild cases) over any field supporting a factoring algorithm,

(4) a precise determination of the maximum number of decompositions of an additive polynomial (which is super-polynomial in the degree), giving a super-polynomial lower bound on the number of decompositions of a given polynomial in the wild case,

(5) a polynomial time algorithm for the complete decomposition of additive polynomials, and hence an algorithm for determining indecomposability,

(6) a quasi-polynomial time algorithm for the decomposition of an additive polynomial into factors of given degrees,

(7) polynomial time algorithms for the decomposition of two special classes of additive polynomials, the completely reducible additive polynomials and the similarity free additive polynomials,

(8) a quasi-polynomial time algorithm for the absolute decomposition of additive polynomials, which could well run in polynomial time, subject to an unproven conjecture of Ore[1933b],

(9) a definition of the rational function decomposition problem, as well as a normalised form of this problem, and a reduction from the general problem to the normal problem,

(10) a computational solution to the normal rational function decomposition problem, requiring an exponential number of field operations.

Results 5 through 8 assume the existence of a polynomial time algorithm for factoring univariate polynomials.

1 Polynomial Decomposition

1.1 Definition of the Problem

Let F be an arbitrary field and K an extension field of F. A *decomposition* of a polynomial $f \in F[x]$ is an ordered sequence of polynomials $f_i \in K[x]$ for $1 \leq i \leq m$ such that

$$\begin{aligned} f &= f_m(f_{m-1}(\cdots(f_2(f_1))\cdots) \\ &= f_m \circ f_{m-1} \circ \cdots \circ f_2 \circ f_1. \end{aligned}$$

If $K = F$ then the decomposition is said to be *rational*. The polynomial f is considered to be *(rationally) indecomposable* if for any (rational) decomposition, all but one of the composition factors has degree one. If this is even true when K is allowed to be an algebraic closure of F, then f is *absolutely indecomposable*.

Assume $f = g \circ h$ where $f \in F[x]$ and $g, h \in K[x]$. Assume also that a and c are the leading (high order) coefficients of f and h respectively. Then

$$\frac{f}{a} = (\frac{1}{a}g(cx + h(0))) \circ \frac{h - h(0)}{c}$$

is a decomposition of a monic polynomial into two monic polynomials, the second of which has constant coefficient zero. Thus, without loss of generality, we can assume for any decomposition $f = g \circ h$ that f, g, and h are monic and $h(0) = 0$. Similarly, if $f = f_m \circ f_{m-1} \circ \cdots \circ f_1$, we can assume that $f \in F[x]$ and $f_i \in K[x]$ for $1 \leq i \leq m$ are monic and $f_i(0) = 0$ for $1 \leq i < m$. Call any decomposition of this form a *normal* decomposition.

Define the *rational normal decomposition problem* as follows. For any $n, m \in \mathbb{N}$, an *ordered factorisation* of n of length m is an m-tuple

$$\wp = (r_m, r_{m-1}, \ldots, r_1)$$

where $r_i \in \mathbb{N}$ and $r_i \geq 2$ for $1 \leq i \leq m$ and

$$\prod_{1 \leq i \leq m} r_i = n.$$

Let $m \in \mathbb{N} \setminus \{0\}$ and let F be any field of characteristic p, where p is a prime number. Let $\mathbb{P}_F = \{f \in F[x] : f \ monic\}$. Define

$$DEC^F_\wp = \left\{ (f, (f_m, f_{m-1}, \ldots, f_1)) \in \mathbb{P}_F \times (\mathbb{P}_F)^m \;\middle|\; \begin{array}{l} f = f_m \circ f_{m-1} \circ \cdots \circ f_1 \\ \text{where } \deg f_i = r_i \text{ and} \\ f_i(0) = 0 \text{ for } 1 \leq i < m \end{array} \right\}.$$

The computational problem is, given $f \in \mathbb{P}_F$ and $\wp$ as above, to decide whether there exist any

$$(f_m, f_{m-1}, \ldots, f_1) \in (\mathbb{P}_F)^m$$

such that

$$(f, (f_m, f_{m-1}, \ldots, f_1)) \in DEC^F_\wp,$$

and in the affirmative case, to compute one or all of them.

The *rational normal bidecomposition problem* is a restriction of the above problem to ordered factorisations $\wp = (r_2, r_1)$ of length two. Mathematically, this problem addresses many of the same questions as the general problem since we can always look at decompositions into two parts, and then continue recursively on the composition factors obtained. This problem has been examined extensively in the literature, but many unresolved questions remain. Two basic cases emerge in the mathematical behaviour of the bidecomposition problem. The "tame" case, when $p \nmid r_2$, is as its name might suggest, well behaved. Kozen and Landau[1986] observed that there exists at most one decomposition for any given f and $\wp$ (this also follows from Fried and MacRae[1969a]). Furthermore, they showed it can be determined in polynomial time. As well, any normal decomposition of f will be rational in this case. This was shown for the case $F = \mathbb{C}$ by Ritt[1922], for all fields of characteristic zero by Levi[1942], and for the general "tame" case by Fried and MacRae[1969a].

The "wild" case, when $p|r_2$, is much harder to deal with, both mathematically and computationally. Fields are exhibited over which the problem is undecidable in von zur Gathen[1988]. Decompositions are not necessarily unique as the following example shows (other examples can be found in Ore[1933b]). Let $F = GF(5)$. Then

$$\begin{aligned} f = x^{5^3} + x^{5^2} + x^5 + x &= (x^{5^2} + 3x^5 + 2x) \circ (x^5 + 3x) \\ &= (x^{5^2} + 4x^5 + 3x) \circ (x^5 + 2x) \\ &= (x^{5^2} + x) \circ (x^5 + x). \end{aligned}$$

Here f has 3 distinct decompositions in $DEC^F_{(5^2,5)}$. Also, in the "wild" case decompositions may not be rational. With F as above consider the polyno-

mial

$$\begin{aligned} f &= x^{5^2} + x^5 + x \\ &= (x^5 + \alpha x) \circ (x^5 + \beta x) \\ &= x^{5^2} + (\beta^5 + \alpha)x^5 + \alpha\beta x. \end{aligned}$$

It follows that $\alpha + \beta^5 = \alpha\beta = 1$, and the polynomial f has a decomposition of this form if and only if β is a root of $\varphi = x^6 - x + 1 \in F[x]$. But φ has no roots in F, and hence f has monic normal decompositions only in algebraic extensions of F. It will be seen that even in small finite fields the number of bidecompositions of a given polynomial of degree n can be super-polynomial in n. Polynomial time decomposition algorithms for rational decompositions and for decompositions in algebraic extensions are known to exist only for certain classes of polynomials.

The ring of polynomials $F[x]$ under addition and composition is obviously without zero divisors. It is not a (left or right) Euclidean ring however, as right or left division with remainder of $f \in F[x]$ by $g \in F[x]$ makes sense only when the degree of g divides the degree of f.

Let $F = GF(4)$, and let $\omega \in F$ be a primitive cube root of unity. Consider the polynomial

$$f = (x^4 - x)^3 \in F[x].$$

Dorey and Whaples[1974] show

$$f = (x^4 - x^3 - x^2 + x) \circ (x^3 + \omega\alpha x + \alpha\omega^2)$$

for any $\alpha \in F$. Hence left (compositional) division of f by $(x^4 - x^3 - x^2 + x)$ is not unique. A somewhat stronger statement can be made about (compositional) right division. Let F be an arbitrary field and K an extension field of F.

Lemma 1.1. *If $f, h \in F[x]$ and $g \in K[x]$ are nonzero of degrees n, r and s respectively, and $f = g \circ h$, then*

(i) g is uniquely determined by f and h, and

(ii) $g \in F[x]$.

Proof.

(i) Assume $g' \in K[x]$ is such that $f = g' \circ h$. Then

$$\begin{aligned} 0 &= g \circ h - g' \circ h \\ &= (g - g') \circ h, \end{aligned}$$

and as $F[x]$ under composition has no zero divisors, this implies that $g = g'$.

(ii) The coefficients of f are K-linear combinations of the coefficients of h^i for $1 \leq i \leq r$. The coefficients of f and h^i are in F, so the coefficients of g are a solution to a system of linear equations over F. Since such a system has a solution in F if it has one over K, and g is unique by (i), the coefficients of g are in F and $g \in F[x]$. □

Further structure can be derived about the fields over which decompositions exist. Let F be a field and let $\bar{F}$ be a fixed algebraic closure of F.

Lemma 1.2. *Let $f, g, h \in F[x]$ have degrees n, r, and s respectively and $f = g \circ h$. Assume f has splitting field $K \subseteq \bar{F}$. Then g splits over K and for each root $\alpha \in K$ of g, $h - \alpha$ splits over K.*

Proof. Assume

$$g = \prod_{1 \leq i \leq r} (x - \beta_i)$$

where $\beta_i \in \bar{F}$ for $1 \leq i \leq r$. Then

$$f = \prod_{1 \leq i \leq r} (h - \beta_i).$$

Let $\gamma = \beta_i$ for some $i \in \mathbb{N}$ with $1 \leq i \leq r$. If $\alpha \in \bar{F}$ is a root of $h - \gamma$, then α is a root of f. Hence $\alpha \in K$ and $h - \gamma$ splits over K. Since γ is the product of the roots of $h - \gamma$, $\gamma \in K$. Therefore, g splits over K as well. □

This theorem implies a number of interesting facts about decompositions over extensions of the ground field.

Corollary 1.3. *Let F be an arbitrary field and $L \supseteq F$ an extension field. Let $f \in F[x]$ be monic of degree n with splitting field K. Then, if f is indecomposable in K, f is indecomposable in L.*

Proof. Suppose $f = g \circ h$ for some $g, h \in L[x]$ whose degrees are at least two. Then, by lemma 1.2, g splits in K, so $g \in K[x]$. Let $\gamma \in K$ be a root of g. Then $h - \gamma$ splits over K (also by lemma 1.2) and $h \in K[x]$. But f is indecomposable over K and we get a contradiction. $\Box$

Decomposition over an arbitrary field extension (or decomposition in the splitting field as just shown) is called *absolute decomposition*. We will see in theorem 2.8 that over many fields F there are polynomials $f \in F[x]$ whose splitting fields are of degree exponential in n over F. Over infinite fields F von zur Gathen [1987a] showed that there exist polynomials of degree n such that the coefficients of an absolute decomposition generate a field extension of degree exponential in n over F. It is conjectured that such examples exist over finite fields as well.

1.2 Decomposition and the Subfields of $F(x)$.

The decompositions of a polynomial $f \in F[x]$ have a strong correspondence with the lattice of subfields between $F(f)$ and $F(x)$, where $F(x)$ is an algebraic extension over $F(f)$ of the same degree as the degree of f (see van der Waerden[1970] section 10.2). This was first examined by Levi[1942] and later by Fried and MacRae[1969a,b]. Let $n \in \mathbb{N}$ and $\wp = (r_m, r_{m-1}, \ldots, r_1)$ be an ordered factorisation of n. Let $\mathbb{L}$ be the set of all subfields of $F(x)$. Define

$$FIELDS_{\wp}^{F} = \left\{ (f, (F_m, \ldots, F_1)) \in \mathbb{P}_F \times \mathbb{L}^m \;\middle|\; \begin{array}{l} F_m = F(f),\ F_0 = F(x), \\ F_m \subseteq F_{m-1} \subseteq \cdots \subseteq F_1 \subseteq F_0, \\ [F_{i-1} : F_i] = r_i,\ 1 \le i \le m \end{array} \right\}$$

where $[F_{i-1} : F_i]$ is the algebraic degree of F_{i-1} over F_i.

Let $f \in F[x]$ be of degree n. Also, let $(f, (f_m, f_{m-1}, \ldots, f_1)) \in DEC_{\wp}^{F}$ and for $1 \le i \le m$ let $h_i = f_i \circ f_{i-1} \circ \cdots f_1$ and $F_i = F(h_i)$, the field F with h_i adjoined. Define $\Gamma_F^D : DEC_{\wp}^{F} \to FIELDS_{\wp}^{F}$ by $(f, (f_m, f_{m-1}, \ldots, f_1)) \mapsto (f, (F_m, F_{m-1}, \ldots, F_1))$. This is a map into $FIELDS_{\wp}^{F}$ by the fact that $[F_{i-1} : F_i] = r_i$.

Theorem 1.4. *Γ_F^D is a bijection.*

Proof. Different decompositions give rise to different chains of fields because for any $h_i, h_i' \in F[x]$, $F(h_i) = F(h_i')$ if and only if $h_i = ah_i' + b$ for some

$a, b \in F$, $a \neq 0$. If $h_i, h_i' \in F[x]$ are monic with $h_i(0) = h_i'(0) = 0$, this implies $h_i = h_i'$. Thus Γ_F^D is injective.

Showing that Γ_F^D is surjective is somewhat less trivial. Let $f \in F[x]$ be monic of degree n. Then $F(x)$ is a finite extension of $F(f)$ of degree n. Let L be a field such that $F(f) \subseteq L \subseteq F(x)$. Then $L = F(h)$ for some $h \in F(x)$. Since h generates L over F and $f \in L$, $f = g \circ h$ for some $g \in F[x]$. Thus h is a root of $f - g(y) \in F(x)[y]$. Since $f - g(y)$ is also in $F[x, y]$, all roots in $F(x)$ must be in $F[x]$ (see van der Waerden[1970] section 5.4) and $h \in F[x]$. As $F(ah + b) = F(h)$ for $a, b \in F$ and $a \neq 0$, we can assume h is monic with $h(0) = 0$. Assume $h' \in F[x]$ is also monic with $h'(0) = 0$ and $L = F(h')$. We know h' and h have the same degree, that is $[F(x) : L]$, and because $h' \in F(h)$, $h' = ch + d$ for some $c, d \in F$, $c \neq 0$. But both are monic with constant coefficient zero, so $h = h'$ and h is unique. Assume h has degree s. The field L is an algebraic extension of $F(f)$ of degree $r = n/s$, and the degree of $g \in F[x]$ is r.

Now assume $(f, (F_m, F_{m-1}, \ldots, F_1)) \in FIELDS_\varphi^F$. Let $h_i \in F[x]$ with $h_i(0) = 0$ be the unique monic generator of F_i as above. Because $F(h_{i-1}) \supseteq F(h_i)$, we know $h_i = f_i \circ h_{i-1}$, for some (unique) $f_i \in F[x]$, for $1 \leq i < m$. The degree of $F(h_{i-1})$ over $F(h_i)$ is r_i, so the degree of f_i is r_i. Because f may have a non-zero constant term, $f = h_m + c$, where $c \in F$ is the constant term of f. As before, $F(h_{m-1}) \supseteq F(h_m)$ so there exists a unique $\bar{f}_m$ of degree r_m such that $h_m = \bar{f}_m \circ h_{m-1}$. Letting $f_m = \bar{f}_m + c$, it follows that $(f, (f_m, f_{m-1}, \ldots, f_1)) \in DEC_\varphi^F$. It is easily seen that $\Gamma_F^D(f, (f_m, f_{m-1}, \ldots, f_1)) = (f, (F_m, F_{m-1}, \ldots, F_1))$ and so Γ_F^D is surjective and hence bijective. □

Let $f \in F[x]$ be separable of degree n (ie. $\frac{\partial}{\partial x} f \neq 0$). In the separable case we can study the lattice of fields between $F(f)$ and $F(x)$ by looking at the Galois group of $F(x)$ relative to $F(f)$. This was first done in Dorey and Whaples[1974] for the set of additive polynomials (a subset of $F[x]$ which will be dealt with in detail in a later section). As $F(x)$ is not necessarily a normal, separable, extension of $F(f)$, we construct the splitting field Ω of the minimal polynomial of x over $F(f)$. This minimal polynomial is

$$\Phi_f(y) = f(y) - f \in F(f)[y] \subseteq F(x)[y] \ ,$$

since we know that x has degree n over $F(f)$ and x satisfies Φ_f which also has degree n. Because f is separable, Φ_f is separable, so the field Ω is a normal,

separable, extension of $F(f)$ containing $F(x)$. Let $\mathcal{G}_f = \mathrm{Gal}(\Omega/F(f))$, the Galois group of Ω relative to $F(f)$, and let $\mathcal{G}_x \subseteq \mathcal{G}_f$ be the subgroup fixing $F(x)$ pointwise. Let $\mathbb{G}$ be the set of all subgroups of $\mathcal{G}_f$. For $n \in \mathbb{N}$ and $\wp = (r_m, r_{m-1}, \ldots, r_1)$, an ordered factorisation of n, define

$$GROUPS^F_\wp = \left\{ (f, (\mathcal{G}_m, \ldots, \mathcal{G}_1)) \in \mathbb{P}_F \times \mathbb{G}^m \;\middle|\; \begin{array}{l} \mathcal{G}_m = \mathcal{G}_f,\ \mathcal{G}_0 = \mathcal{G}_x \\ \mathcal{G}_m \supseteq \mathcal{G}_{m-1} \supseteq \cdots \supseteq \mathcal{G}_1 \supseteq \mathcal{G}_0 \\ (\mathcal{G}_i : \mathcal{G}_{i-1}) = r_i,\ 1 \le i \le r \end{array} \right\}$$

where $(\mathcal{G}_i : \mathcal{G}_{i-1})$ is the index of $\mathcal{G}_{i-1}$ in $\mathcal{G}_i$.

Let $f \in F[x]$ be separable of degree n and let $(f, (F_m, F_{m-1}, \ldots, F_1)) \in FIELDS^F_\wp$. As above, let Ω be the splitting field of Φ_f and let $\mathcal{G}_f = \mathrm{Gal}(\Omega/F(f))$. For $1 \le i \le m$ let $\mathcal{G}_i \subseteq \mathcal{G}_F$ be the group of automorphisms fixing F_i pointwise. Define $\Gamma^F_G : FIELDS^F_\wp \to GROUPS^F_\wp$ by

$$(f, (F_m, F_{m-1}, \ldots, F_1)) \mapsto (f, (\mathcal{G}_m, \mathcal{G}_{m-1} \ldots, \mathcal{G}_1)).$$

This map is simply the one described in the fundamental theorem of Galois theory (see van der Waerden[1970] section 8.1-8.3).

Theorem 1.5. *If f is separable then Γ^F_G is a bijection.*

Proof. By the fundamental theorem of Galois theory, there is an inclusion inverting bijection between fields between $F(x)$ and $F(f)$ and groups between $\mathcal{G}_x$ and $\mathcal{G}_f$. An automorphism group $\mathcal{H}$ such that $\mathcal{G}_x \subseteq \mathcal{H} \subseteq \mathcal{G}_f$ corresponds to the field L such that $F(x) \supseteq L \supseteq F(f)$ which it leaves fixed pointwise. Thus each chain of fields

$$F(f) = F_m \subseteq F_{m-1} \subseteq \cdots \subseteq F_1 \subseteq F(x)$$

corresponds uniquely to a tower of groups

$$\mathcal{G}_f = \mathcal{G}_m \supseteq \mathcal{G}_{m-1} \supseteq \cdots \supseteq \mathcal{G}_0 = \mathcal{G}_x.$$

Also by the fundamental theorem, $(\mathcal{G}_i : \mathcal{G}_{i-1}) = [F_{i-1} : F_i] = r_i$. As Γ^F_G is exactly this Galois mapping, the fact that it is a bijection follows immediately. □

1.3 Separated Polynomials

From the correspondence between decompositions and fields between $F(f)$ and $F(x)$ we get a useful structural result. This was originally due to Fried and MacRae[1969b] and was later extended to the multivariate case by Evyatar and Scott (this will be dealt with in a subsequent section). Fried and MacRae[1969b] introduce a more general version of the polynomials $\Phi_f = f(y) - f(x) \in F(f)[y]$ and $\Phi_h = h(x) - h(y) \in F(h)[y]$ previously described. Let F be an arbitrary field with independent indeterminates x and y over F. A polynomial $\Upsilon \in F[x, y]$ is said to be *separated* if $\Upsilon(x, y) = f_1(x) - f_2(y)$ where $f_1, f_2 \in F[x]$. They then showed the following theorem linking separated polynomials with the simultaneous bidecomposition of two polynomials with a common left composition factor:

Fact 1.6. *Let $f_1, f_2, h_1, h_2 \in F[x]$. Then $h_1(x) - h_2(y) | f_1(x) - f_2(y)$ if and only if there exists a polynomial $g \in F[x]$ such that $f_1 = g \circ h_1$ and $f_2 = g \circ h_2$.*

If we let $f_1 = f_2$ and $h_1 = h_2$ we immediately have the following corollary:

Corollary 1.7. *Let $f, h \in F[x]$ be monic of degrees n and s respectively with $h(0) = 0$. The following are equivalent:*

(i) There exists a $g \in F[x]$ such that $f = g \circ h$.

(ii) $\Phi_h | \Phi_f$.

We can now apply this theorem to get another formulation of general decompositions. Let $\mathbb{S} = \{h(x) - h(y) \in F[x, y] : h \in \mathbb{P}_F\}$. Let $n \in \mathbb{N}$ and $\wp = (r_m, r_{m-1}, \ldots, r_1)$, an ordered factorisation of n. Also, let $d_i = \prod_{1 \leq j \leq i} r_j$. Define

$$SEP^F_\wp = \left\{ (f, (\Phi_m, \Phi_{m-1} \ldots, \Phi_1)) \in \mathbb{P}_F \times \mathbb{S}^m \;\middle|\; \begin{array}{l} \deg_x \Phi_i = d_i,\ \Phi_m = \Phi_f \\ \Phi_i | \Phi_{i+1} \text{ for } 1 \leq i < m \end{array} \right\}.$$

Let $(f, (f_m, f_{m-1}, \ldots, f_1)) \in DEC^F_\wp$ and, for $1 \leq i \leq m$, let

$$u_i = f_i \circ f_{i-1} \circ \cdots \circ f_1(x) - f_i \circ f_{i-1} \circ \cdots \circ f_1(y) \in F[x, y].$$

By corollary 1.7, $u_i | u_{i+1}$. Define the map $\Gamma^D_S : DEC^F_\wp \to SEP^F_\wp$ by

$$(f, (f_m, f_{m-1}, \ldots, f_1)) \mapsto (f, (u_m, u_{m-1} \ldots, u_1)).$$

Theorem 1.8. *Γ_S^D is a bijection.*

Proof. As distinct decompositions will give a distinct sequences of u_i's for $1 \leq i \leq m$, this is an injective mapping from $DEC_\wp^F$ to $SEP_\wp^F$.

Now assume $(f, (v_m, v_{m-1}, \ldots, v_1)) \in SEP_\wp^F$ where $v_i(x, y) = g_i(x) - g_i(y)$ for $1 \leq i \leq m$. By corollary 1.7, we know that for $1 < i \leq m$, $g_i = f_i \circ g_{i-1}$ for some $f_i \in F[x]$ of degree r_i. Thus $(f, (f_m, f_{m-1}, \ldots, f_3, f_2, g_1)) \in DEC_\wp^F$. Each member of $SEP_\wp^F$ will be mapped to a different member of $DEC_\wp^F$ so there is an injection from $SEP_\wp^F$ to $DEC_\wp^F$. This is obviously the inverse of Γ_S^D, and so Γ_S^D is a bijection. $\square$

1.4 Multidimensional Block Decompositions

Kozen and Landau[1986] developed another formulation of the bidecomposition of a polynomial $f \in F[x]$ based on its Galois group G_f, and this group's action on the roots of f in its splitting field. The roots are partitioned by G_f into blocks or systems of imprimitivity (see van der Waerden[1970], section 7.9). A necessary and sufficient condition in terms of these blocks is given for there to be a corresponding bidecomposition of f. We extend this formulation to general decompositions of f corresponding to a given ordered factorisation $\wp$.

Let $\mathcal{U}$ be a set. A *multiset* S over $\mathcal{U}$ is any map $S : \mathcal{U} \to \mathbb{N}$. An element $\alpha \in \mathcal{U}$ is an element of S ($\alpha \in S$) if and only if $S(\alpha) > 0$. A multiset can be viewed as an extension of the characteristic function of a set. A multiset T is a submultiset of a multiset S ($T \subseteq S$) if for all $\alpha \in \mathcal{U}$, $T(\alpha) \leq S(\alpha)$. If $\sigma : \mathcal{U} \to \mathcal{U}$ is a map, we consider the multiset σS to be defined such that for all $\alpha \in \mathcal{U}$

$$(\sigma S)(\alpha) = \sum_{\substack{\beta \in S \\ \sigma\beta = \alpha}} S(\beta).$$

The cardinality of a multiset S is

$$|S| = \sum_{\alpha \in S} S(\alpha).$$

At first reading, the reader is encouraged to think of multisets as sets $S \subseteq \mathcal{U}$ (or equivalently, as the characteristic functions of sets); if the polynomial f to be decomposed is squarefree, indeed only such sets will occur.

We will see that decompositions into, say, three composition factors, correspond in a natural way to certain "multisets of multisets of multisets of roots". We introduce these "typed" objects over some set $\mathcal{U}$ as follows. A *multiset with one level over* $\mathcal{U}$ is a multiset over $\mathcal{U}$ and, for $i > 1$, a *multiset with i levels over* $\mathcal{U}$ is a multiset over the set of multisets with $i-1$ levels over $\mathcal{U}$. Let B be a multiset with m levels over $\mathcal{U}$. A multiset C is a level k member of B if

$$C \in B_{k-1} \in \cdots \in B_1 \in B.$$

Notice that the structure of B implies that C must be a multiset with $m-k$ levels. C also has a natural multiplicity within B, namely

$$B(B_1) \cdot B_1(B_2) \cdots B_{k-2}(B_{k-1}) \cdot B_{k-1}(C).$$

This allows us to "flatten" the top k levels of B and speak of the multiset of all multisets at level ℓ in B. We denote this multiset with $m-k+1$ levels as $B^{[\ell]}$.

Let $m \in \mathbb{N}$ and $\wp = (r_m, r_{m-1}, \ldots, r_1) \in \mathbb{N}^m$. A multiset B with m levels over $\mathcal{U}$ is a $\wp$-*block* if either

(i) $m = 1$ and B is a multiset over $\mathcal{U}$ of cardinality r_1, or

(ii) $m > 1$ and B is a multiset with cardinality r_m of $(r_{m-1}, r_{m-2}, \ldots, r_1)$-blocks over $\mathcal{U}$.

Let $\mathbb{B}_F$ be the set of all multisets with i levels over $\bar{F}$ for all $i > 0$, where $\bar{F}$ is a fixed algebraic closure of F. Define the set

$$BLOCKS_{\wp}^{F} = \left\{ (f, B) \in \mathbb{P}_F \times \mathbb{B}_F \;\middle|\; \begin{array}{c} B \text{ is a } \wp\text{-block over } \bar{F} \text{ such that} \\ f = \prod_{\alpha \in B^{[m]}} (x-\alpha)^{B^{[m]}(\alpha)} \end{array} \right\}.$$

Let $f \in F[x]$ be of degree n with splitting field $K \subseteq \bar{F}$ and Galois group $G_f = \mathrm{Gal}(K/F)$ and let $\wp = (r_m, r_{m-1}, \ldots, r_1)$ be an ordered factorisation of n. A $\wp$-block B over K is a $\wp$-*block decomposition* of f if

(i) $f = \prod_{\alpha \in B^{[m]}} (x-\alpha)^{B^{[m]}(\alpha)}$, and

(ii) for any $\alpha, \beta \in B^{[m]}$ and $\sigma \in G_f$ such that $\sigma\alpha = \beta$, and for $1 \leq \ell < m$ and any C,D over K with $C, D \in B^{[m-\ell]}$ such that $\alpha \in C^{[\ell]}$ and $\beta \in D^{[\ell]}$, it is true that $\sigma C^{[\ell]} = D^{[\ell]}$.

A $\wp$-block decomposition is said to be *functional* if there exist monic polynomials $h_1, h_2, \ldots, h_{m-1} \in F[x]$ such that for $1 \leq \ell < m$, $h_\ell(0) = 0$ and for all $C \in B^{[m-\ell]}$ there exists a $\gamma_C \in K$ such that

$$\prod_{\alpha \in C^{[\ell]}} (x - \alpha)^{C^{[\ell]}(\alpha)} = h_\ell + \gamma_C.$$

Define

$$FBLOCKS^F_\wp = \left\{ (f, B) \in \mathbb{P}_F \times \mathbb{B}_F \;\middle|\; \begin{array}{r} B \text{ is a functional } \wp\text{-block} \\ \text{decomposition of } f \end{array} \right\}.$$

Note that $FBLOCKS^F_\wp \subseteq BLOCKS^F_\wp$.

We now give an example of a $\wp$-block decomposition. Let $p \in \mathbb{N}$ be prime and let $F = GF(p)$. Let $f \in F[x]$ be irreducible of degree $n = 12$ with splitting field $K = F[z]/(f)$ and Galois group $G_f = \mathrm{Gal}(K/F) = \{\sigma_j : x \to x^{p^j} \text{ for } 0 \leq j < 12\}$. We will exhibit a block decomposition of f in $BLOCKS^F_\wp$, where $\wp$ is the ordered factorisation $(2, 3, 2)$. Since F is finite and f is irreducible, f has roots $\{\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{11}}\} \subseteq K$. First, we find a block decomposition B of f in $BLOCKS^F_{(6,2)}$. Let $B = \{C_0, C_1, \ldots, C_5\}$, where $C_i = \{\alpha^{p^i}, \alpha^{p^{i+6}}\}$ for $0 \leq i < 6$. Condition (i) of the definition of a $\wp$-block trivially holds. If, for $0 \leq i, j, k < 12$, $\sigma_k \alpha^{p^i} = \alpha^{p^{i+k}} = \alpha^{p^j}$, then $i + k \equiv j \bmod 12$ and $\sigma_k \alpha^{p^{i+6}} = \alpha^{p^{i+6+k}} = \alpha^{p^{j+6}}$ for $0 \leq i, j, k < 12$ since $i + 6 + k \equiv j + 6 \bmod 12$. Thus, condition (ii) in the definition holds as well. In a similar way we find that $A = \{D_0, D_1\}$ where $D_i = \{\alpha^{2j+i} : 0 \leq j < 5\}$ for $0 \leq i < 2$ is a decomposition of f in $BLOCKS^F_{(2,6)}$. Combining these two decomposition, it follows that

$$E = \left\{ \{\{\alpha, \alpha^{p^6}\}, \{\alpha^{p^2}, \alpha^{p^8}\}, \{\alpha^{p^4}, \alpha^{p^{10}}\}\} \;,\; \{\{\alpha^p, \alpha^{p^7}\}, \{\alpha^{p^3}, \alpha^{p^9}\}, \{\alpha^{p^5}, \alpha^{p^{11}}\}\} \right\}$$

is a block decomposition of f in $BLOCKS^F_{(2,3,2)}$.

We now proceed to describe a bijective map Γ^D_B from $DEC^F_\wp$ to $FBLOCKS^F_\wp$. We first define Γ^D_B from $DEC^F_\wp$ to $BLOCKS^F_\wp$. We then show it is a map to $FBLOCKS^F_\wp$, and finally that it is bijective.

Once again, let $n, m \in \mathbb{N}$ and $\wp = (r_m, r_{m-1}, \ldots, r_1)$, an ordered factorisation of n. Also, let $(f, (f_m, f_{m-1}, \ldots, f_1)) \in DEC^F_\wp$, where $f \in F[x]$ has splitting field K. We define the map Γ^D_B recursively as follows. If $m = 1$, let

B be the multiset of roots of f. It follows immediately that B is a $\wp$-block of the roots of f in K, so we let $\Gamma_B^D(f,(f)) = (f,B)$.

Now assume $m > 1$. We know $f = f_m \circ h_{m-1}$ where $h_\ell = f_{\ell-1} \circ f_{\ell-2} \circ \cdots \circ f_1 \in F[x]$ for $1 \leq \ell \leq m$. Let D_m be the multiset of roots of f_m in K (we know they are in K by lemma 1.2). Then

$$f = \prod_{\alpha \in D_m} (h_{m-1} - \alpha)^{D_m(\alpha)}.$$

For each $\alpha \in D_m$, let $E_\alpha = \Gamma_B^D(h_{m-1} - \alpha, (f_{m-1} - \alpha, f_{m-2}, f_{m-3}, \ldots, f_1))$, an $(r_{m-1}, r_{m-2}, \ldots, r_1)$-block over K of the roots in K of $h_{m-1} - \alpha$ by the recursive definition. For each $(r_{m-1}, r_{m-2}, \ldots, r_1)$-block C over K, define the multiset B such that

$$B(C) = \begin{cases} D_m(\alpha) & \text{if } C = E_\alpha \text{ for some } \alpha \in D_m, \\ 0 & \text{otherwise.} \end{cases}$$

B is the multiset of the E_α's (for all $\alpha \in D_m$) with appropriate multiplicity. This is a $\wp$-block over K of the roots of f and hence $(f,B) \in BLOCKS_\wp^F$. We therefore define $\Gamma_B^D(f,(f_m, f_{m-1}, \ldots, f_1)) = (f,B)$. We have completely described the map $\Gamma_B^D : DEC_\wp^F \to BLOCKS_\wp^F$.

Lemma 1.9. *Γ_B^D is a map from $DEC_\wp^F$ to $FBLOCKS_\wp^F$.*

Proof. Let $(f,(f_m, f_{m-1}, \ldots, f_1)) \in DEC_\wp^F$ and let (f,B) be its image in $BLOCKS_\wp^F$ under Γ_B^D. It follows immediately that (f,B) is functional from the definition of Γ_B^D. We must also show that condition (ii) in the definition of $\wp$-block decomposition holds for (f,B).

Assume $\alpha, \beta \in B^{[m]}$ and $\sigma \in G_f$ such that $\sigma\alpha = \beta$. Let $\ell \in \mathbb{N}$ such that $1 \leq \ell < m$ and let $C, D \in B^{[m-\ell]}$. We know

$$\begin{aligned} \prod_{a \in C^{[\ell]}} (x-a)^{C^{[\ell]}(a)} &= h_\ell + \gamma, \\ \prod_{b \in D^{[\ell]}} (x-b)^{D^{[\ell]}(b)} &= h_\ell + \delta, \end{aligned}$$

for some $\gamma, \delta \in K$ by the definition of Γ_B^D. Since

$$\begin{aligned} 0 &= \sigma(h_\ell(\alpha) + \gamma) \\ &= h_\ell(\sigma\alpha) + \sigma\gamma \\ &= h_\ell(\beta) + \sigma\gamma \end{aligned}$$

and $h_\ell(\beta) + \delta = 0$, we also know $\delta = \sigma\gamma$. Furthermore, since

$$\begin{aligned}\sigma(h_\ell + \gamma) &= \sigma \prod_{a \in C^{[\ell]}} (x-a)^{C^{[\ell]}(a)} \\ &= \prod_{a \in C^{[\ell]}} (x - \sigma a)^{C^{[\ell]}(a)},\end{aligned}$$

and

$$\begin{aligned}\sigma(h_\ell + \gamma) &= h_\ell + \delta \\ &= \prod_{b \in D^{[\ell]}} (x-b)^{D^{[\ell]}(b)},\end{aligned}$$

there is a bijection between the linear factors (over K) of $h_\ell + \gamma$ and $h_\ell + \delta$. As there is a trivial bijection between the linear factors of a polynomial over its splitting field and the multiset of roots of that polynomial, $\sigma C^{[\ell]} = D^{[\ell]}$. Therefore Γ_B^D is a map from $DEC_\wp^F$ to $FBLOCKS_\wp^F$. $\square$

Theorem 1.10. *Γ_B^D is a bijection.*

Proof. Γ_B^D is an injection since each different decomposition gives a different sequence $h_1, h_2, \ldots, h_m$, and hence a different block decomposition. We now show it is also surjective by induction on m. Let $(f, B) \in FBLOCKS_\wp^F$. If $m = 1$ then B is simply the multiset of roots of f and $\Gamma_B^D(f, (f)) = (f, B)$. Assume m is greater than one. Then

$$\begin{aligned}f &= \prod_{\alpha \in B^{[m]}} (x-\alpha)^{B^{[m]}(\alpha)} \\ &= \prod_{D \in B} \Big(\prod_{\alpha \in D^{[m-1]}} (x-\alpha)^{D^{[m-1]}(\alpha)} \Big)^{B(D)} \\ &= \prod_{D \in B} (h_{m-1} - \gamma_D)^{B(D)} \\ &= \prod_{D \in B} (x - \gamma_D)^{B(D)} \circ h_{m-1}\end{aligned}$$

for some $\gamma_D \in K$ for each $D \in B$. It follows that there exists a polynomial $f_m \in K[x]$ such that

$$f_m = \prod_{D \in B} (x - \gamma_D)^{B(D)}$$

and $f = f_m \circ h_{m-1}$. By lemma 1.1, $f_m \in F[x]$ and this f_m is unique. Now let $C \in B^{[m-\ell]}$ for any ℓ with $1 < \ell < m$. Then

$$\begin{aligned}\prod_{\alpha \in C^{[\ell]}} (x-\alpha)^{C^{[\ell]}(\alpha)} &= h_\ell - \delta \quad \text{for some } \delta \in K \\ &= \prod_{D \in C} \Big(\prod_{\alpha \in D^{[\ell-1]}} (x-\alpha)^{D^{[\ell-1]}(\alpha)} \Big)^{C(D)} \\ &= \prod_{D \in C} (h_{\ell-1} - \gamma_D)^{C(D)} \\ &= \prod_{D \in C} (x-\gamma_D)^{C(D)} \circ h_{\ell-1}\end{aligned}$$

for some $\gamma_D \in K$ for each $D \in C$. So there exists a polynomial $g_\ell \in K[x]$ such that

$$g_\ell = \prod_{D \in C} (x-\gamma_D)^{C(D)}$$

and $h_\ell - \delta = g_\ell \circ h_{\ell-1}$. Rearranging this, $h_\ell = (g_\ell + \delta) \circ h_{\ell-1}$ and by lemma 1.1, $f_\ell = g_\ell + \delta \in F[x]$ and this f_ℓ is unique. This shows $h_\ell = f_\ell \circ h_{\ell-1}$ for some uniquely determined $f_\ell \in F[x]$ for $1 < \ell < m$.

It follows that $f = f_m \circ f_{m-1} \circ \cdots \circ f_3 \circ f_2 \circ h_1$ where $f_i \in F[x]$ is monic of degree r_i for $1 < i \leq m$ and $\deg h_1 = r_1$. Therefore $(f, (f_m, f_{m-1}, \ldots, f_3, f_2, h_1)) \in DEC_\wp^F$ and $\Gamma_B^D(f, (f_m, f_{m-1}, \ldots, f_3, f_2, h_1)) = (f, B)$. This means that Γ_B^D is surjective and hence bijective. $\square$

1.5 Chebyshev Polynomials

The Chebyshev polynomials, $T_i \in \mathbb{C}[x]$ for $i \in \mathbb{N}$, are usually defined over the complex numbers by the identity

$$T_i(\cos\theta) = \cos i\theta.$$

From the trigonometric identity

$$\cos\theta_1 + \cos\theta_2 = 2\cos\left(\frac{\theta_1+\theta_2}{2}\right)\cos\left(\frac{\theta_1-\theta_2}{2}\right),$$

we get

$$\cos i\theta + \cos((i-2)\theta) = 2\cos((i-1)\theta)\cos\theta$$

and

$$T_i(\cos\theta) + T_{i-2}(\cos\theta) = 2\cos\theta T_{i-1}(\cos\theta).$$

This gives the defining recurrence relation

$$\begin{aligned} T_0 &= 1, \\ T_1 &= x, \\ T_i &= 2xT_{i-1} - T_{i-2}, \qquad (i > 1) \end{aligned}$$

so that

$$\begin{aligned} T_2 &= 2x^2 - 1, \\ T_3 &= 4x^3 - 3x, \\ T_4 &= 8x^4 - 8x^2 + 1, \\ &\vdots \end{aligned}$$

Note that $T_i \in \mathbb{Z}[x]$ for all $i \in \mathbb{N}$, so Chebyshev polynomials are in fact well defined (by this recurrence) in arbitrary fields of arbitrary characteristic, and have coefficients in the prime field of this characteristic. We will prove a number of useful theorems concerning Chebyshev polynomials over arbitrary fields. Obviously, no analytic properties of trigonometric functions have meaning in fields of positive characteristic, so we will not make use of any of these.

If F has characteristic two, then

$$\begin{aligned} T_0 &= 1, \\ T_1 &= x, \\ T_i &= T_{i-2} \qquad \text{for } i > 2. \end{aligned}$$

Therefore $T_i = 1$ if i is even and $T_i = x$ if i is odd.

Let F be any field of characteristic $p \neq 2$, and for $i \in \mathbb{N}$, let T_i be the i^{th} Chebyshev polynomial. A quick examination of the defining recurrence reveals that $\deg T_i = i$.

Theorem 1.11.

$$T_i\left(\frac{x + x^{-1}}{2}\right) = \frac{x^i + x^{-i}}{2}.$$

Proof. We will proceed by induction on i. Easily, the theorem holds for T_0 and T_1. Assume it holds for T_j with $0 \leq j < i$. Then

$$\begin{aligned} T_i\left(\frac{x+x^{-1}}{2}\right) &= 2 \cdot \frac{x+x^{-1}}{2} \cdot T_{i-1}\left(\frac{x+x^{-1}}{2}\right) - T_{i-2}\left(\frac{x+x^{-1}}{2}\right) \\ &= (x+x^{-1})\left(\frac{x^{i-1}+x^{-(i-1)}}{2}\right) - \frac{x^{i-2}+x^{-(i-2)}}{2} \\ &= \frac{x^i+x^{-i}}{2} \end{aligned}$$

and the theorem holds for all T_i, $i \in \mathbb{N}$. $\square$

Using theorem 1.11, we can show the following fact about the composition of Chebyshev polynomials over arbitrary fields F of characteristic p.

Theorem 1.12. *For $i, j \in \mathbb{N}$, $T_i \circ T_j = T_{ij} = T_j \circ T_i$.*

Proof. If F has characteristic two, then the theorem holds trivially. If the characteristic p of F does not equal two then,

$$\begin{aligned} T_i \circ T_j\left(\frac{x+x^{-1}}{2}\right) &= T_i\left(\frac{x^j+x^{-j}}{2}\right) \\ &= \frac{x^{ij}+x^{-ij}}{2} \\ &= T_{ij}\left(\frac{x+x^{-1}}{2}\right) \end{aligned}$$

From this identity in $F(x)$, we conclude that $T_i \circ T_j = T_{ij}$. $\square$

In fields of characteristic $p > 2$, a useful theorem can be shown about the Chebyshev polynomials of degree p^i for $i \geq 1$.

Theorem 1.13. *Let F be any field of characteristic $p > 2$. For $i \in \mathbb{N}$, $T_{p^i} = x^{p^i}$.*

Proof. By theorem 1.12,

$$T_{p^i} = \overbrace{T_p \circ T_p \circ \cdots \circ T_p}^{i \text{ times}}$$

so it is sufficient to show $T_p = x^p$. We know

$$T_p\left(\frac{x+x^{-1}}{2}\right) = \frac{x^p + x^{-p}}{2} = \left(\frac{x+x^{-1}}{2}\right)^p.$$

From this identity in $F(x)$, we conclude that $T_p = x^p$. $\square$

1.6 Complete Rational Decompositions

A *complete* rational decomposition of a polynomial $f \in F[x]$ is of the form

$$f = f_m \circ f_{m-1} \circ \cdots \circ f_2 \circ f_1$$

where each $f_i \in F[x]$ is indecomposable and nontrivial (ie. with degree greater than one). A natural question to ask concerns the uniqueness of such decompositions. As we do not want to worry about affine linear transformations of composition factors, we consider only complete rational normal decompositions where f is monic and $f_i \in F[x]$ are monic for $1 \leq i \leq m$ and $f_i(0) = 0$ for $1 \leq i < m$.

Two types of ambiguous decompositions emerge. If $u \in F[x]$, then $(x^m \cdot u^r) \circ x^r = x^r \circ (x^m \cdot u(x^r))$ for $m, r \in \mathbb{N}$. Call this an *exponential* ambiguity. As seen in the previous section, the Chebyshev polynomials $T_i \in F[x]$ for $i \in \mathbb{N}$ have the property that $T_i \circ T_j = T_j \circ T_i$. Call this a *trigonometric* ambiguity. Ritt[1922] showed that if $F = \mathbb{C}$, all complete normal decompositions differ only by ambiguities of these two forms. Engstrom[1941] showed that in fields F of characteristic zero that

(i) polynomials indecomposable over F are indecomposable over any algebraic extension of F (ie. all decompositions are rational), and

(ii) all complete normal decompositions differ only by trigonometric and exponential ambiguities.

These two theorems are known as Ritt's first and second theorems. Fried and MacRae[1969a] showed them true when the characteristic of F is greater than the degree of the polynomial.

For an arbitrary field F of characteristic p this is not necessarily true. Dorey and Whaples[1974] give the following example of two complete rational decompositions of the polynomial $f \in F[x]$:

$$\begin{aligned} f &= x^{p^3+p^2} - x^{p^3+1} - x^{p^2+p} + x^{p+1} \\ &= x^{p+1} \circ (x^p + x) \circ (x^p - x) \\ &= (x^{p^2} - x^{p^2-p+1} - x^p + x) \circ x^{p+1}. \end{aligned}$$

The composition factor $x^{p^2} - x^{p^2-p+1} - x^p + x$ is indecomposable because the composition of two polynomials of degree p can never have a term of degree $p^2 - p + 1$.

The various equivalent formulations to polynomial decompositions can be extended to complete decompositions in the obvious manner. Let $\wp$ be an ordered factorisation of n of length m. Let $cDEC^F_\wp \subseteq DEC^F_\wp$ be the set of complete decompositions of polynomials corresponding to ordered factorisation $\wp$. The image of $cDEC^F_\wp$ in $FIELDS^F_\wp$, $GROUPS^F_\wp$, $SEP^F_\wp$, and $FBLOCKS^F_\wp$ under the bijections described in this chapter will be called, respectively, $cFIELDS^F_\wp$, $cGROUPS^F_\wp$, $cSEP^F_\wp$ and $cBLOCKS^F_\wp$. Obviously, any member of any one of these sets will correspond to a complete rational normal decomposition.

The sets $cFIELDS^F_\wp$ and $cGROUPS^F_\wp$ have useful characterisations in their own right. If $(f, (F_m, F_{m-1}, \ldots, F_1)) \in cFIELDS^F_\wp$, then

$$F(f) = F_m \subseteq F_{m-1} \subseteq \cdots \subseteq F_1 \subseteq F(x)$$

is a maximal chain of fields. If a field did exist between F_i and F_{i+1} then f_{i+1}, the $i+1$'st composition factor from the corresponding element $(f, (f_m, f_{m-1}, \ldots, f_1)) \in cDEC^F_\wp$, would be decomposable. In a similar fashion, if $(f, (\mathcal{G}_m, \mathcal{G}_{m-1}, \ldots, \mathcal{G}_1)) \in cGROUPS^F_\wp$, then

$$\mathcal{G}_x \subseteq \mathcal{G}_1 \subseteq \cdots \subseteq \mathcal{G}_{m-1} \subseteq \mathcal{G}_m = \mathcal{G}_f$$

is a maximal tower of groups.

When dealing with complete decompositions of a polynomial $f \in F[x]$, we often wish to deal with all decompositions of f regardless of the ordered factorisations to which they correspond. With this in mind we define

$$cDEC^F_* = \bigcup_{\wp \in \mathbb{T}} cDEC^F_\wp.$$

where $\mathbb{T}$ is the set of all finite tuples of integers greater than one. Similarly we can define $cFIELDS_*^F$, $cGROUPS_*^F$, etc, and restate Ritt's second theorem in this context: For any monic $f \in F[x]$, all decompositions of f in $cDEC_*^F$ are equivalent up to trigonometric and exponential ambiguities.

1.7 The Number of Indecomposable Polynomials

It can shown that "most" polynomials over an arbitrary field F are indecomposable. This can be done using an algebraic dimension argument over an algebraically closed field and by a counting argument over a finite field.

Let F be a field, and $\mathbb{M} \subseteq F[x]$ be the set of monic polynomials with constant coefficient zero. Also, for $n \in \mathbb{N}$, let $\mathbb{M}_n = \{f \in \mathbb{M} \mid \deg f = n\}$ and for $r, s \in \mathbb{N}$ with $rs = n$ and $g \in \mathbb{M}_r$ and $h \in \mathbb{M}_s$, define $\alpha_{(r,s)} : \mathbb{M}_r \times \mathbb{M}_s \to \mathbb{M}_{rs}$ by $\alpha_{(r,s)}(g, h) = g \circ h$ (ie. the composition function). Assume $f = \sum_{0 \le i \le n} a_i x^i \in \mathbb{M}_n$ where $a_i \in F$ for $0 \le i \le n$. We define the map $\lambda_n : \mathbb{M}_n \to F^{n-1}$ by $\lambda_n(f) = (a_{n-1}, a_{n-2}, \ldots, a_1)$. This is obviously a bijective map from $\mathbb{M}_n$ to F^{n-1}. Assume r and s are at least two and define $\beta_{(r,s)} : F^{r-1} \times F^{s-1} \to F^{n-1}$ by $\beta_{(r,s)} = \lambda_n \circ \alpha_{(r,s)} \circ (\lambda_r^{-1} \times \lambda_s^{-1})$. This is the composition map in F^{n-1}. Let

$$D_{(r,s)} = \{\beta_{(r,s)}(A, B) \in F^{n-1} \mid A \in F^{r-1},\ B \in F^{s-1}\}$$

be the image of $\beta_{(r,s)}$ in F^{n-1}. We will show that the "size" of F^{n-1} is "much larger" than the "size" of

$$D = \bigcup_{rs=n} D_{(r,s)},$$

the set of all decomposable polynomials in $\mathbb{M}_n$. Because we can normalise any decomposition, this is in fact a general statement about the number of indecomposable polynomials in $F[x]$.

Consider the case where F is an algebraically closed field. For $r, s \in \mathbb{N}$ with $rs = n$ and $r > 1$, $\bar{D}_{(r,s)}$ (the Zariski closure of $D_{(r,s)}$) is an algebraic set of dimension at most $r + s - 2$. Therefore

$$\bar{D} = \bigcup_{\substack{rs=n \\ r,s>1}} \bar{D}_{(r,s)}$$

has dimension at most

$$\max\{\dim \bar{D}_{(r,s)} \ :\ rs = n,\ r, s > 2\} \le \frac{n}{2}$$

and this is less than the dimension $n-1$ of F^{n-1}. Therefore, over an arbitrary infinite field, "most" polynomials are indecomposable even over an algebraic closure of that field, in a strong algebraic sense.

Turning to the case $F = GF(q)$ where $q = p^i$ for some prime number p and $i \in \mathbb{N}$, we can make a counting argument to show that only an exponentially small number of polynomials in $F[x]$ of degree n are decomposable. For any ordered factorisation (r, s) of n with $s > 1$, we know $\#D_{(r,s)} \leq q^{r-1}q^{s-1} = q^{r+s-2}$. Summing over all possible ordered factorisation (r, s) of n where $s > 1$, we get

$$\begin{aligned}\#D &\leq \sum_{rs=n} q^{r+s-2} \\ &\leq d(n)q^{2+n/2-2}\,. \\ &\leq d(n)q^{n/2}\end{aligned}$$

where $d(n)$ is the number of divisors of n. From Hardy and Wright[1960] (theorem 317) we get $d(n) \leq c_\epsilon n^\epsilon$ for any $\epsilon > 0$ and some $c_\epsilon > 0$ (depending on ϵ). Fixing an $\epsilon > 0$,

$$\begin{aligned}\#D &\leq c_\epsilon q^{\frac{n}{2}} \\ &\leq c_\epsilon q^{\epsilon \log_q n + \frac{n}{2}} \\ &\leq kq^{2n/3}.\end{aligned}$$

for some $k > 0$. This shows that only an exponentially small fraction of the polynomials of degree n over $GF(q)$ are decomposable.

1.8 Multivariate Decomposition

Let F be an arbitrary field and let $x, x_1, \ldots, x_\ell, y, y_1, \ldots, y_\ell$ be algebraically independent indeterminates over F for $\ell \in \mathbb{N} \setminus \{0\}$. For convenience we write the sequences $x_1, \ldots, x_\ell$ and $y_1, \ldots, y_\ell$ as $\vec{x}$ and $\vec{y}$ respectively. For $f \in F[\vec{x}]$, let $\deg f$ be the total degree of f. We will simply refer to this as the degree of f. For $f \in F[\vec{x}]$ of degree n, a decomposition of f is a pair $(g, h) \in F[x] \times F[\vec{x}]$ such that $f = g \circ h$. Note that if g has degree r and h has degree s, then f has degree $n = rs$. For any $\alpha \in F$, we have $f = [g \circ (x + \alpha)] \circ [(x - \alpha) \circ h]$ so we can assume $h(0, \ldots, 0) = 0$. Let (r, s) be an ordered factorisation of n. For any positive integer ℓ, define the set

$$MDEC^{F,\ell}_{(r,s)} = \left\{ (f, (g, h)) \in F[\vec{x}] \times (F[x] \times F[\vec{x}]) \;\middle|\; \begin{array}{r} f = g \circ h,\ \deg g = r, \\ \deg h = s, h(0, \ldots, 0) = 0 \end{array} \right\}.$$

If $(f,(g,h)) \in MDEC^{F,\ell}_{(r,s)}$ then for any $\alpha \in F$, $(f,(g(\alpha x),\alpha^{-1}h)) \in MDEC^{F,\ell}_{(r,s)}$. We say the two decompositions $(f,(g,h))$, and $(f,(g(\alpha x),\alpha^{-1}h))$ are *linearly equivalent*. Removing linearly equivalent decompositions from $MDEC^{F,\ell}_{(r,s)}$ and choosing a canonical representative from each equivalence class is not as natural as in the univariate case and will not be attempted here. Two different approaches to this problem will be presented when dealing with multivariate decompositions algorithmically. As in the univariate case we define the tame case to be when $p \nmid r$. In von zur Gathen [1987b] it is shown that in the tame case for any $f \in F[x]$ of degree n and any ordered factorisation (r,s) of n, all decompositions of f (if any) in $MDEC^{F,\ell}_{(r,s)}$ are linearly equivalent.

Evyatar and Scott[1972] show the following multivariate generalisation of the Fried and MacRae[1968a] theorem concerning separated polynomials (see section 1.C).

Fact 1.14. *If $f,h \in F[\vec{x}]$ then there exists a $g \in F[x]$ such that $f = g \circ h$ if and only if $h(\vec{x}) - h(\vec{y}) | f(\vec{x}) - f(\vec{y})$.*

Define the set $\mathbb{W}_\ell = \{h(\vec{x}) - h(\vec{y}) | h \in F[\vec{x}]\}$. Also define

$$MSEP^{F,\ell}_{(r,s)} = \left\{ (f,(\Phi,\Psi)) \in F[\vec{x}] \times (\mathbb{W}_\ell)^2 \;\middle|\; \begin{array}{c} \Phi = f(\vec{x}) - f(\vec{y}),\ \Psi | \Phi, \\ \deg \Phi = rs,\ \deg \Psi = r \end{array} \right\}.$$

Considering fact 1.14, there is a map $\Gamma^{MD}_{MS} : MDEC^{F,\ell}_{(r,s)} \to MSEP^{F,\ell}_{(r,s)}$. Namely, for $(f,(g,h)) \in MDEC^{F,\ell}_{(r,s)}$, $(f,(g,h)) \mapsto (f,(f(\vec{x}) - f(\vec{y}), h(\vec{x}) - h(\vec{y})))$.

Theorem 1.15. *Γ^{MD}_{MS} is a bijection.*

Proof. Assume $f,h \in F[\vec{x}]$ and $g,g' \in F[x]$ where $h \neq 0$ and $f = g \circ h = g' \circ h$. Then $g \circ h - g' \circ h = (g - g') \circ h = 0$ and $g - g' = 0$. Thus g is uniquely determined by f and h and Γ^{MD}_{MS} is injective. Conversely, if $(f,(f(\vec{x}) - f(\vec{y}), h(\vec{x}) - h(\vec{y}))) \in MSEP^{F,\ell}_{(r,s)}$, then by fact 1.14 there exists a $g \in F[x]$ such that $f = g \circ h$ and the inverse map is also injective. Therefore, Γ^{MD}_{MS} is a bijection. $\square$

2 Decomposition Algorithms

The development of algorithms for the decomposition of polynomials has occurred relatively recently. Although related problems for power series were examined by Brent and Kung[1976,1977], polynomial decomposition algorithms (for univariate polynomials) were not truly examined until Barton and Zippel[1976,1985]. Their algorithms require an exponential number of field operations (in the degree of the input polynomial) and work over any field which supports a factoring algorithm. Alagar and Thanh[1986] showed a similar algorithm which also requires an exponential number of field operations. The breakthrough came when Kozen and Landau[1986] developed a decomposition algorithm for the tame case which required a polynomial number of field operations (in the degree of the input polynomial) as well as giving a fast parallel algorithm. In von zur Gathen[1987] this result for the tame case was improved, and a very fast parallel algorithm was developed. Kozen and Landau[1986] also show a decomposition algorithm for the general univariate case based on block decomposition, for fields supporting a polynomial factorisation algorithm. This algorithm requires an exponential number of field operations in the degree of the input polynomial, plus the cost of factoring the input polynomial. For separable irreducible polynomials over arbitrary fields their algorithm is shown to work in a quasi-polynomial number of field operations. And for irreducible polynomials over finite fields, their algorithm requires only a polynomial number of field operations. All this is reported in von zur Gathen, Kozen, and Landau[1987]. Complete decompositions are dealt with in the tame case in von zur Gathen[1987]. We also consider computing decompositions of polynomials corresponding to a given ordered factorisation of their degrees.

Multivariate polynomial decomposition in the tame case was examined by Dickerson[1987] and von zur Gathen[1987]. Both showed algorithms requiring a polynomial number of field operations (in the size of the input polynomial): Dickerson[1987] for the "monic" tame case and von zur Gathen[1987] for the tame case in general. We present an algorithm for multivariate decomposition over any field supporting a univariate polynomial factoring algorithm, based on the theorem of Evyatar and Scott[1982] and the univariate algorithm of Barton and Zippel[1985]. In general, it will require an exponential number of field operations.

2.1 The Model of Computation

The model of computation used is the "arithmetic Boolean circuit" (see von zur Gathen [1986]). This model uses inputs $x_1, x_2, \ldots, x_n$ from a field F. Operations are the arithmetic (field) operations $+$, $-$, $\times$, $/$, and Boolean operations $\wedge$, $\vee$, and $\neg$. The connection between the arithmetic and Boolean parts of the circuit is provided by two types of gates. The zero test gate gives a Boolean indication of whether or not an input field value is zero. The selection gate outputs one of two input field values depending upon the value of a third, Boolean, input. The cost of algorithms will be measured in the number of field operations performed. Often, the input will be a polynomial $f \in F[x]$ and the number of field operations will be counted in terms of the degree n of f and the characteristic p of F. If $F = GF(p^e)$ for some $e \geq 1$, we will also consider the cost of computation over the prime field $\mathbb{Z}_p$, and hence in terms of e as well.

Assume we can factor an arbitrary univariate polynomial $f \in F[x]$ of degree n into irreducible factors in $O(\mathbf{S}_F(n))$ field operations. Then we can also factor a multivariate polynomial $g \in F[x_1, x_2, \ldots, x_\ell]$ of total degree n into irreducible factors. Assume this can be accomplished in $O(\mathbf{S}_F^{(\ell)}(n))$ field operations (where $\mathbf{S}_F^{(\ell)}(n)$ is a function of the size $(n+1)^\ell$ of a dense representation of the input). Let $M(n)$ be such that the product of two polynomials of degree at most n can be computed in $O(M(n))$ field operations. We can choose $M(n) = n \log n \log\log n$ (Schönhage[1977], Cantor and Kaltofen[1987]), and $M(n) = n \log n$ if F supports a Fast Fourier Transform. Also, assume two $n \times n$ matrices can be multiplied in $O(n^\mu)$ field operations for some $\mu > 2$. Coppersmith and Winograd[1987] show $\mu < 2.38$.

In some of our algorithms we use $\mathbf{P}(S)$ to denote the set of all subsets (the power set) of a set S, and S^* to denote the set of finite sequences of elements of S.

2.2 Computing Right Division

Given $f, h \in F[x]$ of degrees n and s respectively with $s|n$, we would like to determine if there is a $g \in K[x]$, where K is some algebraic extension of F, such that $f = g \circ h$. Lemma 1.1 shows us that if such a $g \in K[x]$ exists it will be in $F[x]$. We find g by the usual divide and conquer approach, which is used in von zur Gathen [1987b].

RightDivide: $F[x] \times F[x] \to F[x]$
Input: - $f, h \in F[x]$ of degrees n and s respectively, with $s|n$.
Output: - $g \in F[x]$ of degree r such that $f = g \circ h$ if such a g exists.
If $\deg f \leq 0$
then return $f \in F$.
Else if $0 < \deg f < \deg h$
then Quit (there is no solution).
Else if $\deg h \leq \deg f$,
1) Let $t := \lceil r/2 \rceil$.
2) Let $v := h^t$.
3) Find $Q, R \in F[x]$ such that $f = Qv + R$ with $\deg R < \deg v$.
4) Recursively call RightDivide on (R, h) yielding $g_0 \in F[x]$ and (Q, h) yielding $g_1 \in F[x]$.
5) Return $g_1 x^t + g_0$.

This algorithm requires $O(M(n) \log n)$ field operations, with step two the dominant step at each recursive stage of the algorithm. We have the following:

Theorem 2.1. *Given $f, h \in F[x]$, we can determine if there exists a $g \in F[x]$ such that $f = g \circ h$ and if so, find it in $O(M(n) \log n)$ field operations.*

2.3 Univariate Decomposition using Separated Polynomials

The algorithm of Barton and Zippel[1985] exploits the relationship between separated polynomials and polynomial decompositions described in section 1.C. Let F be an arbitrary field of characteristic p. Let $f \in F[x]$ be of degree n and let $(r, s) \in \mathbb{N}^2$ be an ordered factorisation of n. We present a modified version of the Barton and Zippel[1985] algorithm conforming to our definition of the problem.

SepBidecomp : $F[x] \times \mathbb{N}^2 \to DEC^F_*$
Input: - $f \in F[x]$ monic of degree n.
- $(r, s) \in \mathbb{N}^2$, an ordered factorisation of n.
Output: - $(g, h) \in F[x]$ such that $(f, (g, h)) \in DEC^F_{(r,s)}$ if such a decomposition exists.

1) Factor $f(x) - f(0) = xq_1(x)q_2(x)\cdots q_m(x)$
   where each $q_i \in F[x]$ is irreducible for $1 \le i \le m$.

2) For each subset S of $\{1, \ldots, m\}$,

   2.1) Let $h = x\prod_{i\in S} q_i \in F[x]$.

   2.2) If $\deg h = s$, attempt to compute $g \in F[x]$ such that
   $f = g \circ h$ using RightDivide. If such a g is found, then goto step 4.

3) Quit, f has no decomposition in $DEC^F_{(r,s)}$.

4) Return $(f, (g, h)) \in DEC^F_{(r,s)}$.

By theorem 1.6, for any polynomials $f, h \in F[x]$, there exists a $g \in F[x]$ such that $f = g \circ h$ if and only if $h(x) - h(y) | f(x) - f(y)$. Thus, $h(x) - h(0) | f(x) - f(0)$. By looking at all factors h of $f(x) - f(0)$, we are guaranteed to find all possible right composition factors. Since there are 2^n subsets which must be checked for separation in step 2, the algorithm requires $O(\mathbf{S}_F(n) + 2^n M(n) \log n)$ field operations. It does, however, work over any field for which a factorisation algorithm exists (in both the tame and wild cases).

2.4 Univariate Decomposition in the Tame Case

Kozen and Landau [1986] present an algorithm for univariate decomposition in the tame case over an arbitrary field, which uses a polynomial number of field operations in the degree of the input polynomial. For $f \in F[x]$ of degree n, they look at the decompositions of f into (g, h) as solutions to systems of $n+1$ non-linear equations for the coefficients of f in terms of the coefficients of g and h.

Specifically, for $u \in F[x]$ and $i \in \mathbb{N}$, let $\text{coeff}(u, i) \in F$ be the coefficient

of x^i in u. Let

$$\begin{aligned}
f &= \sum_{0\le i\le n} a_i x^i \in F[x] && \text{with } a_i \in F \text{ for } 0 \le i \le n,\\
g &= \sum_{0\le i\le r} b_i x^i \in F[x] && \text{with } b_i \in F \text{ for } 0 \le i \le r,\\
h &= \sum_{1\le i\le s} c_i x^i \in F[x] && \text{with } c_i \in F \text{ for } 1 \le i \le s,\\
\mu_k &= \sum_{s-k+1\le i\le s} c_i x^i \in F[x] && \text{with } c_i \in F \text{ for } s-k+1 \le i \le s \text{ and } 1 \le k \le s.
\end{aligned}$$

If $f = g \circ h$, the following facts are easily seen to be true:

(i) $\text{coeff}(h^r, n-e) = \text{coeff}(f, n-e) = a_{n-e}$ for $0 < e < s$,
(ii) $\text{coeff}(h^r, n-e) = \text{coeff}(\mu_k^r, n-e)$ for $e < k \le s$.

This implies $a_{n-e} = \text{coeff}(f, n-e) = \text{coeff}(\mu_k^r, n-e)$ for $e < k \le s$. For $1 \le k < s$, we know $\mu_{k+1} = \mu_k + c_{s-k}x^{s-k}$. By binomial expansion we get

$$\begin{aligned}
\mu_{k+1}^r &= (\mu_k + c_{s-k}x^{s-k})^r\\
&= \mu_k^r + rc_{s-k}x^{s-k}\mu_k^{r-1} + \varphi,
\end{aligned}$$

where $\varphi \in F[x]$ and $\deg\varphi \le rs - 2k$. Thus $\text{coeff}(\mu_{k+1}^r, rs-k) = a_{rs-k} = \text{coeff}(\mu_k^r, rs-k) + rc_{s-k}$. This gives the simple recurrence

$$c_{s-k} = \frac{a_{rs-k} - \text{coeff}(\mu_k^r, rs-k)}{r},$$

which allows the computation of $c_s, c_{s-1}, \ldots, c_1$ in turn, and hence the calculation of h. Note that it is at this point, and only this point, that we require that $p \nmid r$. This distinguishes the tame and wild cases.

This system of equations uniquely determines an $h \in F[x]$ but a $g \in F[x]$ such that $f = g \circ h$ may or may not exist. We can determine the existence of such a g, and if it exists, find it, using `RightDivide` as described earlier. Kozen and Landau[1986] show that a decomposition can be computed in $O(n^3)$ field operations in general and $O(n^2 \log n)$ field operations in a field which supports a Fast Fourier Transform. In fact, the algorithm works over any ring in which r is a unit.

In von zur Gathen[1987], an improvement of the result of Kozen and Landau[1986] is shown. Given a monic $f \in F[x]$ of degree n and (r, s) an

ordered factorisation of n with $p \nmid r$, his algorithm determines if there exists a decomposition of f in $DEC^F_{(r,s)}$ and, if so, finds it, in $O(M(n)\log n)$ field operations. The number of field operations required is dominated by the cost of `RightDivide` to obtain g from f and h. Von zur Gathen[1987] uses this algorithm for decomposition to obtain the set of separated factors of a given polynomial $f \in F[x]$ of degree n in polynomial time in the tame case.

A very fast parallel algorithm is also presented by von zur Gathen[1987] for univariate bidecomposition in the tame case. He shows that over any field F, given $f \in F[x]$ and (r,s), an ordered factorisation of n such that $p \nmid r$, it can be determined if there exists a decomposition of f in $DEC^F_{(r,s)}$, and if so, it can be found, with a depth $O(\log n)$ circuit over F.

2.5 Decomposition using Block Decomposition

As seen in section 1.D, the polynomial decomposition problem can be reformulated as one of finding functional block decompositions. Let $f \in F[x]$ be monic of degree n, and (r,s) an ordered factorisation of n. Kozen and Landau[1987] adapt the techniques from Landau and Miller[1983] to construct all block decompositions of dimension two of f in $BLOCKS^F_{(r,s)}$. They then check each such decomposition to see if it is functional. In general, however, their algorithm requires a number of field operations exponential in n. If f is separable and irreducible over F, they show that there can be at most $n^{\log n}$ block decompositions in $BLOCKS^F_{(r,s)}$, and that each block decomposition can be constructed in a polynomial number of field operations. Testing a block decomposition to see if it is functional requires only a polynomial number of field operations, but we may have to check all of them. Therefore, for separable irreducible polynomials $f \in F[x]$, it can be determined if f has a decomposition in $DEC^F_{(r,s)}$, and if so, this decomposition can be found, in a quasi-polynomial number ($n^{O(\log n)}$) of field operations over F.

The block decompositions of irreducible polynomials over a finite field $F = GF(q)$ (where $q = p^e$ for some $e \geq 1$) have a stronger structure. Let $f \in F[x]$ of degree n be irreducible with splitting field $K = F[x]/(f)$, and let (r,s) be an ordered factorisation of n. The roots of f in K have the form $\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}\}$ for any one root $\alpha \in K$ of f. The Galois group of K relative to F is the set of automorphisms $\{\sigma_i : 0 \leq i < r\}$ with $\sigma_i\gamma = \gamma^{q^i}$ for any $\gamma \in K$. Kozen and Landau[1986] note that the only possible block decomposition of f has the form $B = \{C_i | 0 \leq i < r\}$ where

$C_i = \{\alpha^{q^{i+jr}} | 0 \leq j < s\}$ for $0 \leq i < r$. It is functional (and hence corresponds to a polynomial decomposition) if and only if there exists an $h \in F[x]$ such that for $0 \leq i < r$, there exists a $\gamma_i \in K$ such that

$$\prod_{0 \leq j < s} (x - \alpha^{q^{i+jr}}) = h - \gamma_i.$$

The splitting field K of f is an algebraic extension of degree n over F, so we can easily compute a representation of these roots (in K), and check if this block decomposition is functional in a polynomial number of field operations. Kozen and Landau[1986] show that in this case, it can be determined if a polynomial f has a bidecomposition in $DEC^F_{(r,s)}$, and if so, this decomposition can be found, with a circuit of depth $O(\log epn \log^2 n)$ and size $(epn)^{O(1)}$. We show the sequential analysis of this algorithm in the following theorem.

Theorem 2.2. *Let $F = GF(q)$ for some $q, p, e \in \mathbb{N}$ with p prime and $q = p^e$, and let $f \in F[x]$ be irreducible of degree n. If (r, s) is an ordered factorisation of n we can determine if there exists a decomposition of f in $DEC^F_{(r,s)}$, and if so, find it, in $O(n^2 M(n) \log q)$ field operations over F.*

Proof. Let $K = F[z]/(f)$ and let $\alpha \equiv z \bmod f \in K$. Multiplication in K requires $O(M(n))$ field operations in F. We can therefore compute $\alpha^{q^{ri}}$ for all i with $0 \leq i < s$ with

$$\begin{aligned} \sum_{0 \leq i < s} ri \log q &= O(rs^2 \log q) \\ &= O(n^2 \log q) \end{aligned}$$

field operations over K or $O(n^2 M(n) \log q)$ field operations over F. We then check if $\prod_{0 \leq i < s}(x - \alpha^{q^{ri}}) = h + c$ where $h \in F[x]$ and $c \in K$. If so, there exists a g such that $(f, (g, h)) \in DEC^F_{(r,s)}$ and this can be found in $O(M(n) \log n)$ field operations by theorem 2.1. We can compute $\prod_{0 \leq i < s}(x - \alpha^{q^{ri}})$ in $O(n^2)$ field operation over K or $O(n^2 M(n))$ field operation over F. Therefore the bidecomposition problem can be solved sequentially for irreducible polynomials over finite fields with $O(n^2 M(n) \log q)$ field operations over F. □

2.6 A Lower Bound on the Degrees of Splitting Fields

Let F be a field such that for any $m \in \mathbb{N}$, there exists an algebraic extension of F of degree m over F. We will now show that in any such field, for any $n \in \mathbb{N}$,

there exist polynomials of degree n over F with splitting fields of degree exponential in n over F. Note in particular that finite fields are included in this theorem. One implication of this is that we cannot construct a standard representation of elements of such a splitting field in a polynomial number of field operations. It has been known for a long time that over the rationals and some other infinite fields that for any n, there exist polynomials of degree n whose Galois groups are S_n. The splitting fields of these polynomials are of algebraic degree $n!$ over their ground fields. In general however, such polynomials do not exist (see van der Waerden section 8.10, Jacobson section 4.10). We instead make the following construction in an arbitrary field F. Let $p_i \in \mathbb{N}$ be the i^{th} smallest rational prime. Also define

$$\vartheta(\ell) = \sum_{\substack{p \text{ prime} \\ p \le \ell}} \log p \quad \text{the Chebyshev } \vartheta \text{ function,}$$
$$\pi(\ell) = \sum_{\substack{p \text{ prime} \\ p \le \ell}} 1$$

(where all logarithms here and throughout this section are natural). Let $f_i \in F[x]$ be an irreducible polynomial of degree p_i. The splitting field K_i of f_i has degree at least p_i over F. If F is a finite field, $[K_i : F] = p_i$. The polynomial $h_i = f_1 f_2 \ldots f_i$ will have splitting field L_i generated by the elements of $K_1 \cup K_2 \cup \cdots \cup K_i$. This is a field of algebraic degree at least $p_1 p_2 \ldots p_i$ over F. Let

$$S(\ell) = \sum_{\substack{p \text{ prime} \\ p \le \ell}} p,$$
$$R(\ell) = \prod_{\substack{p \text{ prime} \\ p \le \ell}} p.$$

Note that $R(\ell) = \exp(\vartheta(\ell))$.

Let $n \in \mathbb{N}$. If $k = \max\{i \,|\, p_i \le \ell\}$, then h_k has a splitting field of degree $R(\ell)$ over F. We will show that if $\ell \le 0.77\sqrt{n \log n}$, then $\deg h_k = S(\ell) \le n$. It follows that $R(0.77\sqrt{n \log n})$ is exponential in n. If $f \in F[x]$ is any polynomial of degree n with divisor h_k, we show that f has a splitting field of degree at least $\exp(0.5\sqrt{n \log n})$ over F. We will use the following bounds from Rosser and Schoenfeld[1962]:

Fact 2.3.

(i) $p_k < 1.4k \log k$ *for* $k \geq 6$*;*

(ii) $\pi(\ell) \leq 1.26\ell / \log \ell$ *for* $\ell \geq 17$*;*

(iii) $\ell(1 - 1/\log \ell) < \vartheta(\ell)$ *for* $n \geq 41$*.*

First, we show an upper bound on the function $\sigma(k) = S(p_k) = \sum_{1 \leq i \leq k} p_i$, the sum of the first k primes, for $k \in \mathbb{N}$.

Lemma 2.4. *For* $k \geq 6$, $\sigma(k) \leq 0.86k^2 \log k$

Proof.

$$\begin{aligned}
\sigma(k) &\leq 2 + 3 + 5 + 7 + 11 + 1.4 \sum_{6 \leq i \leq k} i \log i \\
&\leq 28 + 1.4 \int_6^k (i+1) \log(i+1) di \\
&\leq 28 + 1.4(0.5(i+1)^2 \log(i+1) - 0.25(i+1)^2 \Big|_6^k) \\
&\leq 0.86k^2 \log k \qquad \square
\end{aligned}$$

Lemma 2.5. *For any* $n \geq 109$, $S(0.77\sqrt{n \log n}) \leq n$.

Proof. Applying lemma 2.4 to the the upper bound on the number of primes less than ℓ provided by fact 2.3(ii),

$$\begin{aligned}
S(\ell) &\leq 0.86 \left(\frac{1.26\ell}{\log \ell} \right)^2 \log \left(\frac{1.26\ell}{\log \ell} \right) \\
&\leq 0.86(1.26)^2 \frac{\ell^2}{(\log \ell)^2} (\log(1.26\ell) - \log \log \ell) \\
&\leq 1.37 \frac{\ell^2}{(\log \ell)^2} (\log \ell + \log 1.26 - \log \log \ell) \\
&\leq \frac{1.7\ell^2}{\log \ell}
\end{aligned}$$

for $\ell \geq 17$. For $n \geq 109$ this gives us

$$S(0.77\sqrt{n \log n}) \leq \frac{1.7(0.77\sqrt{n \log n})^2}{\log(0.77\sqrt{n \log n})} \leq \frac{n}{\log(0.77\sqrt{n \log n})} \leq n,$$

and the lemma follows. $\square$

Theorem 2.6. *For $n \geq 109$ there exists a polynomial $f \in F[x]$ of degree n such that the splitting field of f has degree over F greater than $\exp(0.5\sqrt{n \log n})$.*

Proof. By lemma 2.5, if $\ell \leq 0.77\sqrt{n \log n}$, then $S(\ell) \leq n$. Let $\ell = \lfloor 0.77\sqrt{n \log n} \rfloor$. Let $k = \max\{i | \, p_i \leq \ell\}$. The polynomial h_k has a splitting field L_k with degree at least $R(\ell)$. By definition

$$\begin{aligned} R(\ell) &= \exp(\vartheta(\ell)) \\ &\geq \exp(\ell(1 - 1/\log \ell)) \\ &\geq \exp(0.77\sqrt{n \log n}(1 - 1/\log(0.77\sqrt{n \log n}))) \\ &\geq \exp(0.5\sqrt{n \log n}), \end{aligned}$$

for $n \geq 109$. Therefore h_k has a splitting field of degree at least $\exp(0.5\sqrt{n \log n})$. Let f be any polynomial of degree n such that h_k divides f (h_k has degree less than n). The polynomial f has a splitting field of degree at least $\exp(0.5\sqrt{n \log n})$ over F. $\square$

2.7 Decompositions Corresponding To Ordered Factorisations

Let $f \in F[x]$ be of degree n and let $\wp = (r_m, r_{m-1}, \ldots, r_1)$ be an ordered factorisation of n. A natural generalisation of the computational bidecomposition problem is to compute the decompositions of f in $DEC^F_\wp$ (if any). Let `GenericBidecomp` be an algorithm such that given $f \in F[x]$ of degree n, and $(r, s) \in \mathbb{N}^2$, an ordered factorisation of n, it will find the (possibly empty) set B of decompositions of f in $DEC^F_{(r,s)}$ using $D(n)$ field operations. Consider the following algorithm:

`OrdFactDecomp:` $F[x] \times \mathbf{P}(\mathbb{N}) \to \mathbf{P}(DEC^F_*)$
`Input:` - $f \in F[x]$ `of degree` n,
- $\wp = (r_m, r_{m-1}, \ldots, r_1)$, `an ordered factorisation of` n.
`Output:` - `the set of decompositions of` f `in` $DEC^F_\wp$.
`If` $m = 1$
`then return` $(f, (f))$
`else`
`1) Find the set` B `of bidecompositions` $(f, (g, h)) \in DEC^F_{(t_2, r_1)}$

```
      where t_2 = ∏_{2≤i≤m} r_i,
      using GenericBidecomp.
2) Let T := ∅.
3) For each decomposition (f,(g,h)) ∈ B,
      3.1) Recursively attempt to
           find a decomposition
           (g,(g_m,g_{m-1},...,g_2)) ∈ DEC^F_{(r_m,r_{m-1},...,r_2)}.
      3.2) If such a decomposition of g is found
           add (f,(g_m,g_{m-1},...,g_2,h)) to T.
4) Return T.
```

This is simply a recursive application of the bidecomposition algorithm, and can easily be seen to return the set of decompositions of f in $DEC^F_\wp$.

We now define a $\wp$-*easy* family of polynomials, a family in which such decompositions can be computed quickly. For $1 \leq i \leq m$, let $\wp_i = (r_m, r_{m-1}, \ldots, r_i)$ and $t_i = \prod_{i \leq j \leq m} r_j$. A set $\mathcal{F}_\wp \subseteq F[x]$ is $\wp$-*easy* if

(i) for any i with $1 \leq i < m$, any $f \in \mathcal{F}_\wp$ of degree d has at most one decomposition in $DEC^F_{(t_{i+1}, r_i)}$,

(ii) it can be determined if such a decomposition exists, and if it does, it can be found with $O(D(d)) = d^{O(1)}$ field operations, and

(iii) if $f \in \mathcal{F}_\wp$ and $(f,(g,h)) \in DEC^F_{(t_{i+1}, r_i)}$ then $g \in \mathcal{F}_\wp$.

If $\mathcal{F}_\wp \subseteq F[x]$ is a $\wp$-easy family of polynomials, then the bidecompositions of $f \in \mathcal{F}_\wp$ in step 1 can be found in $D(n)$ field operations. Thus, computing `OrdFactDecomp` on $f \in \mathcal{F}_\wp$ with ordered factorisation $\wp$ requires $O(\sum_{1 \leq i < m} D(t_i))$ field operations. Let $\ell = \lceil \log_2 n \rceil$ and let $\kappa = (e_\ell, e_{\ell-1}, \ldots, e_1)$, where $e_i = 2^i$ for $1 \leq i \leq \ell$. Noting that $n \leq \ell < 2n$, it follows immediately that $e_{\ell-j} \geq f_{m-j}$ for $0 \leq j < m$. Therefore $\sum_{1 \leq i < m} D(t_i) \leq \sum_{1 \leq i < \ell} D(e_i)$. Since D is polynomially bounded, $\sum_{1 \leq i < \ell} D(e_i) = O(D(n))$. We have shown the following theorem:

Theorem 2.7. *Let $n \in \mathbb{N}$ and let $\wp$ be an ordered factorisation of n. Also, let $\mathcal{F}_\wp \subseteq F[x]$ be $\wp$-easy. Then, for any $f \in \mathcal{F}_\wp$, we can determine if there exists a decomposition of f in $DEC^F_\wp$, and if so, find it, in $O(D(n))$ field operations.*

This theorem says that the general problem of computing the set of decompositions of a polynomial with a given ordered factorisation is Cook reducible to the bidecomposition problem for $\wp$-easy families of polynomials.

Two $\wp$-easy families present themselves immediately. If F is an arbitrary field and $p \nmid r_i$ for $1 < i \leq m$ then $F[x]$ is a $\wp$-easy family of polynomials. This follows because all the bidecompositions performed in step 1 are tame. From von zur Gathen[1987] and theorem 2.7 above, it can be determined whether a decomposition of $f \in F[x]$ exists in $DEC^F_\wp$ and if so such a decomposition can be found in $O(M(n)\log n)$ field operations.

If $F = GF(q)$ and $\mathcal{F}_\wp$ is the set of polynomials irreducible over F, then $\mathcal{F}_\wp$ is $\wp$-easy. This follows since, if $f \in \mathcal{F}_\wp$ and $(f,(g,h)) \in DEC^F_*$, then g is also irreducible over F. By theorem 2.2 and theorem 2.7, a decomposition of any $f \in \mathcal{F}_\wp$ can be found in $O(n^2 M(n)\log q)$ field operations.

2.8 Computing Complete Univariate Decompositions

The following method for computing complete decompositions was suggested in von zur Gathen[1987] for the tame case and can be applied whenever we can do bidecomposition. Let $D(n)$ be the number of field operations required to find a bidecomposition of $f \in F[x]$ corresponding to an ordered factorisation (r,s) of n. The following algorithm computes a complete decomposition of f in DEC^F_*.

`CompleteDecomposition:` $\mathbb{P}_F \rightarrow cDEC^F_*$
`Input:` - $f \in F[x]$.
`Output:` - $(f,(f_m,f_{m-1},\ldots,f_1)) \in cDEC^F_*$.
`1)` Compute the integer factorisation $n = p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$ of n.
`2)` Let $d(n) = (e_1+1)\cdots(e_k+1)$ be the number of divisors of n and $1 = r_1 < r_2 < \cdots < r_{d(n)} = n$ be the divisors of n.
`3)` Let $j > 1$ be the smallest number such that f has a decomposition $(f,(g,h)) \in DEC^F_{(r_j,n/r_j)}$.
`4)` If $j = d(n)$ then f is indecomposable; otherwise decompose h recursively (g is indecomposable since any left composition factor of g is a composition factor of f of smaller degree than g).

The number of field operations required by this algorithm is $O(D(n)d(n))$. Hardy and Wright[1960] (theorem 317) show that $d(n) = O(n^\epsilon)$ for all $\epsilon >$

0. Therefore, we can compute complete decompositions in $O(D(n)n^{\epsilon})$ field operations for any $\epsilon > 0$. This algorithm finds the *lexicographically first complete decomposition* of f.

2.9 Decomposing Multivariate Polynomials in the Tame Case

Once again we denote the sequence of indeterminates $x_1, \ldots, x_\ell$ as $\vec{x}$. We define the set $\mathbb{W}_F^{(\ell)} \subseteq F[\vec{x}]$ of *monic* polynomials in $F[\vec{x}]$ as follows:

$$\mathbb{W}_F^{(\ell)} = \left\{ f = x_1^{d_1} x_2^{d_2} \cdots x_\ell^{d_\ell} + \hat{f} \;\middle|\; \begin{array}{l} \hat{f} \in F[\vec{x}],\ \deg \hat{f} < \deg f \\ d_i \in \mathbb{N} \setminus \{0\},\ \deg_{x_i} \hat{f} \leq d_i \text{ for } 1 \leq i \leq \ell \end{array} \right\}$$

where $\deg f$ and $\deg \hat{f}$ are the total degrees of f and $\hat{f}$ respectively. Dickerson[1987] uses much the same method as Kozen and Landau[1986] did for the univariate case to decompose monic multivariate polynomials in the tame case. Given a monic $f \in F[\vec{x}]$ of degree n and $r \in \mathbb{N}$, he shows how to find a monic $g \in F[x]$ of degree r and monic $h \in F[\vec{x}]$ of degree $r = n/s$ such that $f = g \circ h$. The computation requires $O(n^{3\ell})$ field operations. From the algorithm it is seen that if such a decomposition exists, it is unique. Note that monic multivariate polynomials are a very special case of multivariate polynomials. Just because they can be decomposed does not mean that multivariate polynomials can be decomposed in the tame case in general (though it is possible a reduction from the general case exists).

In von zur Gathen[1987], the tame case for the decomposition of multivariate polynomials is dealt with completely. He first defines the set of polynomials $\mathbb{P}_F^{(\ell)} \subseteq F[\vec{x}]$ which are *strongly monic* in x_1 as follows:

$$\mathbb{P}_F^{(\ell)} = \left\{ f = \sum_{0 \leq i \leq n} f_i x_1^i \in F[\vec{x}] \;\middle|\; \begin{array}{l} n \in \mathbb{N},\ f_0, \ldots, f_n \in F[x_2, \ldots, x_\ell] \\ f_n = 1,\ \deg f = n \end{array} \right\}.$$

If $f \in F[\vec{x}]$ is strongly monic and $f = g \circ h$, then $f(x_1, 0, \ldots, 0) = g \circ h(x_1, 0, \ldots, 0)$. As we know $f(x_1, 0, \ldots, 0)$ is of degree n (f is strongly monic), the univariate decomposition of $f(x_1, 0, \ldots, 0)$ in $DEC_{(r,s)}^F$ completely determines $g \in F[x]$ in the multivariate decomposition. Once g is computed, a linearly convergent Newton iteration is used to compute $h \in F[\vec{x}]$ in a number of field operations polynomial in the input size. Given $f \in F[\vec{x}]$ and

$g \in F[x]$, the process of finding $h \in F[\vec{x}]$ such that $f = g \circ h$ is a special case of (multivariate) power series reversion. This is dealt with extensively by Brent and Kung[1977,1978]. They show the problem is linearly equivalent to power series composition when $(\partial g/\partial x) \neq 0$, which is true in the tame case. Furthermore, they show that multivariate polynomial reversion can be computed in $O((n \log n)^{\frac{1}{2}} M(n)^{\ell})$ field operations.

For an arbitrary $f \in F[\vec{x}]$ we can use substitutions of the form $\sigma(x_i) = x_i + \sigma_i x_1$ with $x_i \in F$ for $2 \leq i \leq m$ to make f strongly monic. For such a substitution σ we write $\sigma f = f(x_1, x_2 + \sigma_2 x_1, \ldots, x_m + \sigma_m x_1)$. This substitution σ may be inverted by the substitution $\sigma^{-1} = (-\sigma_2, -\sigma_3, \ldots, -\sigma_m)$ and $\sigma\sigma^{-1} f = f$. For a suitably chosen substitution σ, $\bar{f} = a\sigma f$ is strongly monic in x_1 (where $a \in F$ is chosen to make the highest order coefficient of x_1 in $a\sigma f$ one). If $\bar{f} = \bar{g} \circ \bar{h}$ for $\bar{g}, \bar{h} \in F[x]$ then $f = (a^{-1}\bar{g}) \circ (\sigma^{-1}\bar{h})$ is a corresponding decomposition of f.

For $f \in F[\vec{x}]$ of total degree n, von zur Gathen[1987] shows how to choose a substitution σ such that σf is strongly monic. This can be done in a polynomial number of field operations in m, n, and k, where k is the number of monomials in f. (the sparse representation of f has size $O(km \log n)$). For $0 \leq i \leq n$, let $u_i \in F[x_2, \ldots, x_m]$ be the homogenous part of degree $n - i$ of the coefficient of x_1^i in f. The homogenous part of degree n of f is therefore $\sum_{0 \leq i \leq n} u_i x^i \neq 0$, and by the homogeneity of the u_i's, $u = \sum_{0 \leq i \leq n} u_i$ is also nonzero, and of degree at most n. Let K be an extension field of F with more than n points. K can be chosen as a field of degree $O(\log n)$ over F. Now, for a substitution $\sigma = (\sigma_2, \sigma_3, \ldots, \sigma_m)$, $\deg_{x_1} \sigma f = n$ if and only if

$$\deg f(x_1, \sigma_2 x_1, \ldots, \sigma_m x_1) = \deg[(\sigma)(x_1, 0, \ldots, 0)] = n.$$

This is true if and only if $u(\sigma_2, \sigma_3, \ldots, \sigma_m) \neq 0$. To find $\sigma_2, \ldots, \sigma_m$ we proceed in stages i from 2 to m. At stage i we choose $\sigma_i \in K$ such that

$$u(\sigma_2, \ldots, \sigma_i, x_{i+1}, \ldots, x_m)$$

is nonzero. We do this by considering $v_i = u(\sigma_2, \ldots, \sigma_{i-1}, x_i, \ldots, x_m)$ as a polynomial in $K(x_{i+1}, \ldots, x_m)[x_i]$ of degree in x_i at most n. Thus v_i has at most n roots in $K(x_{i+1}, \ldots, x_m)$ and we can find a non-root $\sigma_i \in K$ of v_i with at most n evaluations of v_i at points in K. Assume f is the sum of at most k monomials. Then u is also the sum of at most k monomials and σ can be found in $O(kmn \log n)$ field operations over K or $O(kmn \log n M(\log n))$

field operations over F. Decomposing multivariate polynomials is, therefore, polynomial time (in the input degree and the size of the sparse representation) reducible to decomposing strongly monic multivariate polynomials.

2.10 Multivariate Decomposition Using Separated Polynomials

Using theorem 1.15 we can generalise the algorithm of Barton and Zippel[1985] to the multivariate case and obtain a multivariate decomposition algorithm for any field supporting a factorisation algorithm. To do this we must show a "right division" algorithm for the multivariate case. Namely, given $f, h \in F[\vec{x}]$, we must be able to find a $g \in F[x]$ such that $f = g \circ h$ (if such a g exists). We cannot use the "Taylor Expansion" method of the univariate case directly. Instead we use the methods of von zur Gathen[1987] to transform the problem to one involving strongly monic polynomials. Another simple transformation yields a univariate problem such that the solution is the same as in the original problem.

`MultiRightDivide:` $F[\vec{x}] \times F[\vec{x}] \to F[x]$
`Input:` - $f, h \in F[\vec{x}]$ `of total degrees` n `and` s `respectively.`
`Output:` - $g \in F[x]$ `of degree` $r = n/s$ `such that` $f = g \circ h$
(`if such a` g `exists`).
1) `Let` K `be an algebraic extension of` F `with more than` n `elements.`
`Let` $\sigma = (\sigma_2, \sigma_3, \ldots, \sigma_m) \in K^{m-1}$
`be a substitution and` $a \in K$ `such that`
$\bar{f} = a\sigma f = f(x_1, x_2 + \sigma_2 x_1, \ldots, x_m + \sigma_m x_1) \in K[x]$
`is strongly monic (see previous section).`
2) `Let` $\bar{h} = \sigma h$.
3) `Using RightDivide determine if there exists a` $\bar{g} \in K[x]$
`such that` $\bar{f}(x, 0, \ldots, 0) = \bar{g} \circ \bar{h}(x, 0, \ldots, 0)$
`and if so find it. If no such` $\bar{g}$ `exists, quit.`
4) `Return` $g = a^{-1}\bar{g}$.

In the previous section we saw that step 1 can be performed in $O(kmn \log nM(\log n))$ field operations over F, where k is the number of monomials in f. It follows that $f = g \circ h$ if and only if $a\sigma f = ag \circ \sigma h$. Since $a\sigma f$ is strongly monic, there exists a $g \in F[x]$ such that $a\sigma f = ag \circ \sigma h$ if and only if $a\sigma f(x, 0, \ldots, 0) = ag \circ \sigma h(x, 0, \ldots, 0)$. Using `RightDivide` we can

determine the existence of $\bar{g} = ag$, and if it exists find it, in $O(M(n)\log n)$ field operations over K or $O(M(n)\log nM(\log n))$ field operations over F. If $\bar{g}$ exists we can immediately compute g, and the whole computation requires $O((kmn\log n + M(n)\log n)M(\log n))$ field operations over F

The algorithm for multivariate decomposition over any field supporting a factorisation algorithm proceeds in much the same way as the Barton and Zippel[1985] algorithm for the univariate case.

`MultiSepDecomp :` $F[\vec{x}] \times \mathbb{N}^2 \to MDEC^F_*$

`Input:` - $f \in F[\vec{x}]$ `of degree` n
- $(r,s) \in \mathbb{N}^2$`, an ordered factorisation of` n

`Output:` - $(g,h) \in (F[x] \times F[\vec{x}])$ `such that` $f = g \circ h$ `if such a decomposition exists`

`1) Factor` $f(\vec{x}) - f(0,\ldots,0) = \vec{x}q_1(\vec{x})q_2(\vec{x})\cdots q_m(\vec{x})$ `where each` $q_i \in F[\vec{x}]$ `is irreducible for` $1 \le i \le m$

`2) For each subset` S `of` $\{1,\ldots,m\}$

`2.1) Let` $h = \vec{x}\prod_{i\in S} q_i \in F[\vec{x}]$.

`2.2) If` $\deg h = s$`, attempt to compute` $g \in F[x]$ `such that` $f = g \circ h$ `using MultiRightDivide. If such a` g `is found, then goto step 4.`

`3) Quit,` f `has no decomposition in` $MDEC^F_{(r,s)}$.

`4) Return` $(f,(g,h)) \in MDEC^F_{(r,s)}$.

The number of subsets of S is 2^n. This algorithm can, therefore, be completed with $O(\mathbf{S}_F(n) + 2^n(kmn\log n + M(n)\log n)M(\log n))$ field operations over F. It does, however, work in both the tame and wild cases over any field supporting a polynomial factorisation algorithm.

3 Additive Polynomials

3.1 Definition and Root Structure of Additive Polynomials

Let F be an arbitrary field of characteristic p greater than zero. Define a polynomial $f \in F[x]$ to be an *additive polynomial* if, for independent indeterminates x and y,

$$f(x+y) = f(x) + f(y).$$

The non-zero additive polynomials in $F[x]$ are exactly those of the form

$$f = \sum_{0 \le i \le \nu} a_i x^{p^i}$$

where $\nu \in \mathbb{N}$, $a_i \in F$ for $1 \le i \le \nu$, and $a_\nu \neq 0$. The integer ν is called the *exponent* of f, and we write "expn $f = \nu$". We denote the set of additive polynomials over F as $\mathbb{A}_F$.

The additive polynomials have a well understood decomposition structure which leads to a number of interesting results on decomposition in the general case. This structure was first developed in Ore[1933b], who investigated the vector space structure of the roots of additive polynomials (as well as investigating the ring structure of the additive polynomials under composition – see chapter 4). This work was continued by Whaples[1954], who examined the Galois groups of additive polynomials and characterised additive polynomials in terms of these groups. In Dorey and Whaples, the Galois group $\mathcal{G}_f$ of $\Phi_f = f - f(x) \in F(f)[y]$ (where $f \in \mathbb{A}_F$) is used (see section 1.B) to show that all normal decompositions of additive polynomials are decompositions into additive polynomials. We use this approach to develop much of the structure of the roots of additive polynomials in terms of $\mathcal{G}_f$. Though the theorems in this section are for the most part known (with the possible exception of theorem 3.2(i)), the extension of the approach of Dorey and Whaples is of interest. For a given additive polynomial $f \in \mathbb{A}_F$, it serves to illustrate the strong connection between the separated factors of Φ_f, the Galois structure of f (which is the basis for block decompositions), and the Galois structure of Φ_f. Not coincidentally, each of these three approaches leads to at least one algorithm – the first being the separated polynomial algorithms of Barton and Zippel and Alagar and Thanh, the second being the block decomposition algorithm of Kozen and Landau, and the last being a number of algorithms specifically for additive polynomials, which are presented in chapter 5.

Theorem 3.1.

(i) Let $f \in \mathbb{A}_F$ be monic, with exponent ν such that f is squarefree ($a_0 = f'(0) \neq 0$). Let K be the splitting field of f. Then the roots of f in K form a vector space V_f over $\mathbb{Z}_p$ of dimension ν.

(ii) For each finite $\mathbb{Z}_p$-vector space $V \subseteq F$ of dimension ν, there exists a unique monic $f \in \mathbb{A}_F$ with exponent ν such that the roots of f are exactly the elements of V.

Proof.

(i) For $\alpha, \beta \in K$ such that $f(\alpha) = f(\beta) = 0$, we see that

$$\begin{aligned} f(\alpha + \beta) &= f(\alpha) + f(\beta) = 0, \\ f(k\alpha) &= kf(\alpha) = 0 \qquad\qquad \text{for any } k \in \mathbb{Z}_p. \end{aligned}$$

Since $f'(0) \neq 0$, the greatest common divisor of f and f' is one, and hence f has no multiple roots. Therefore V_f has p^ν distinct elements and dimension ν.

(ii) Let $(\theta_1, \ldots, \theta_\nu)$ be a basis for V in F over $\mathbb{Z}_p$. The polynomial

$$\Psi_1 = x^p - \theta_1^{p-1} x \in \mathbb{A}_F$$

has roots $k\theta_1$ for all $k \in \mathbb{Z}_p$. For $i \geq 2$, define

$$\Psi_i = (x^p - \Psi_{i-1}(\theta_i)^{p-1} x) \circ \Psi_{i-1} \in \mathbb{A}_F.$$

If $\Psi_{i-1}(\alpha) = 0$ for $\alpha \in F$ then $\Psi_i(\alpha) = 0$. Also,

$$\Psi_i(\theta_i) = \Psi_{i-1}(\theta_i)^p - \Psi_{i-1}(\theta_i)^{p-1} \Psi_{i-1}(\theta_i) = 0.$$

Since Ψ_i is additive, Ψ_i has roots consisting of all $\mathbb{Z}_p$-linear combinations of $\{\theta_1, \ldots, \theta_i\}$. Thus the roots of Ψ_i are exactly the members of the vector space with basis $(\theta_1, \ldots, \theta_i)$. Let $f = \Psi_n$, which is monic and additive. This f is also unique by virtue of being a monic interpolant of degree p^ν of p^ν distinct points. Note also that $f'(0) \neq 0$ as f has p^ν distinct roots in f and degree p^ν.

Call the $\mathbb{Z}_p$-vector space V of roots of an additive polynomial $f \in F[x]$ the *kernel* of f. Say an additive polynomial is *simple* if it is monic and $f'(0) \neq 0$. In this section we will deal almost exclusively with simple additive polynomials. Non-simple monic additive polynomials are just simple polynomials composed on the right with x^{p^ℓ} for some $\ell > 0$. Assume $f \in \mathbb{A}_F$ is monic and $f = g \circ x^{p^\ell} \in \mathbb{A}_F$ where $g \in \mathbb{A}_F$ is simple and

$$g = \sum_{0 \leq i \leq \sigma} b_i x^{p^i}$$

with $\sigma \in \mathbb{N}$, $b_i \in F$, and $b_\sigma \neq 0$. Then

$$\begin{aligned} f &= \sum_{0 \leq i \leq \sigma} b_i x^{p^{i+\ell}} \\ &= x^{p^\ell} \circ \sum_{0 \leq i \leq \sigma} (b_i)^{\frac{1}{p^\ell}} x^{p^i} \\ &= x^{p^\ell} \circ \bar{g} \end{aligned}$$

where

$$\bar{g} = \sum_{0 \leq i \leq \sigma} (b_i)^{\frac{1}{p^\ell}} x^{p^i} \in \mathbb{A}_K$$

and K is an algebraic extension of F. So f has a kernel of dimension σ, namely the kernel of $\bar{g}$. If F is perfect (and hence closed under p^{th} roots) $\bar{g}$ will be in $F[x]$ as well.

Let $f \in \mathbb{A}_F$ be simple with exponent ν, splitting field K and kernel $V_f \subseteq K$. The structure of the kernel of f and that of the fields between $K(f)$ and $K(x)$ (and hence the structure of the decompositions of f over its splitting field) are closely linked. Let $\Phi_f = f(y) - f \in F(f)[y] \subseteq F(x)[y]$ with splitting field $\Omega \supseteq F(f)$ and Galois group $\mathcal{G}_f = Gal(\Omega/F(f))$ as in theorem 1.5. Because $\frac{\partial}{\partial y}\Phi_f = \frac{\partial}{\partial y} f(y) \neq 0$, Ω is a separable field extension of $F(f)$.

Theorem 3.2.

(i) $K(x)$ *is the splitting field of* Φ_f,

(ii) $\mathcal{G}_f$ *is the group* $\{x \mapsto x+\alpha \mid \alpha \in K,\ f(\alpha) = 0\}$ *under composition, and*

(iii) $V_f \cong \mathcal{G}_f$.

Proof.

(i) For $\alpha \in V_f$,

$$\begin{aligned}\Phi_f(x+\alpha) &= f(x+\alpha) - f(x) \\ &= f(x) + f(\alpha) - f(x) \\ &= 0.\end{aligned}$$

Since Φ_f has degree p^ν over $F(f)$, $x + V_f$ is the complete set of roots of Φ_f. We know that $x \in x + V_f$ and K is the smallest extension field of F containing V_f, so $\Omega = K(x)$.

(ii) From (i), all roots of Φ_f are of the form $x + \alpha$ where α is a root of f in K. Therefore, $\mathcal{G}_f$ contains the p^ν automorphisms $\{x \mapsto x + \alpha \mid \alpha \in K \ , \ f(\alpha) = 0\}$. Since $[F(x) : F(f)] = p^\nu$, this is the entire Galois group.

(iii) From (ii), $\mathcal{G}_f$ is isomorphic to a set of monic linear elements in $K[x]$ under composition. Trivially this is isomorphic to the group of constant terms of these elements under addition. These constant terms are all the roots of f in K, so $\mathcal{G}_f \cong V_f$. $\square$

Theorem 3.3. *Let $f \in \mathbb{A}_F$ be simple of exponent ν. Let $g, h \in F[x]$ be of degrees $r = p^\rho$ and $s = p^\sigma$ respectively such that $(f, (g, h)) \in DEC^F_{(r,s)}$. Then*

(i) g and h are additive and simple, and

(ii) h has kernel $V_h \cong \mathcal{G}_h$, where $\mathcal{G}_h \subseteq \mathcal{G}_f$ is the subgroup fixing $F(h) \subseteq F(x)$ pointwise.

Proof. By theorem 1.5, the automorphisms in $\mathcal{G}_f$ fixing $F(h)$ form a group $\mathcal{G}_h$ such that $\mathcal{G}_x \subseteq \mathcal{G}_h \subseteq \mathcal{G}_f$, and the index of $\mathcal{G}_x$ in $\mathcal{G}_h$ is p^σ. From theorem 3.2(i), $K(x)$ is the splitting field of Φ_f, so $\mathcal{G}_x$ is the identity group, and the cardinality of $\mathcal{G}_h$ is p^σ. From the isomorphism between $\mathcal{G}_f$ and V_f, there is a subspace W of V_f of dimension σ corresponding to the subgroup $\mathcal{G}_h$. Let $\bar{h} \in K[x]$ be the simple additive polynomial with kernel W. For all $\alpha \in W$, $\bar{h}(x + \alpha) = \bar{h}(x) + \bar{h}(\alpha) = \bar{h}(x)$. Thus $F(\bar{h})$ is fixed by $\mathcal{G}_h$. By theorem 3.1, $\bar{h}$ is unique, so $\bar{h} = h$. Now, for algebraically independent indeterminates x and y, $f = g(h(x + y)) = g(h(x) + h(y))$ and since f is

additive $f = g(h(x)) + g(h(y))$. Thus g is monic and additive. If g is not simple then $g = \bar{g} \circ x^{p^\ell}$ for some simple additive polynomial $\bar{g} \in K[x]$ and $\ell > 0$. But then $f = \bar{g} \circ x^{p^\ell} \circ h = \bar{g} \circ h^{p^l}$ which is not simple. So g is simple as well. □

3.2 Rationality and the Kernel

If $f \in \mathbb{A}_F$ is simple with kernel $V_f \subseteq K$ and splitting field K, a subspace $V_h \subseteq V_f$ is said to be *rational* if the simple polynomial $h \in \mathbb{A}_K$ corresponding to V_h is in $\mathbb{A}_F$. We would also like to formulate rationality in terms of the structure of the kernel.

Theorem 3.4. *A subspace V_h of V_f is rational if and only if V_h is invariant (as a set) under $G_f = \mathrm{Gal}(K/F)$.*

Proof. Assume $h \in \mathbb{A}_F$. The coefficients of h are the values of the elementary symmetric functions of the roots of h in K. The automorphisms in G_f leave these coefficients fixed, and must therefore leave V_h invariant (as a set).

Conversely, if V_h is invariant under G_f then the values of the elementary symmetric functions of the elements of V_h are fixed under G_f, and so are in F. These are exactly the coefficients of h and so $h \in \mathbb{A}_F$. □

When dealing with a finite field F a somewhat stronger structure can be shown.

Theorem 3.5. *Let $F = GF(q)$ where $q = p^e \in \mathbb{N}$ for some $p, e \in \mathbb{N}$ with p prime. Let K be an algebraic extension of F and $f \in \mathbb{A}_K$ of exponent ν with kernel V_f and splitting field L. Then $f \in \mathbb{A}_F$ if and only if $V_f^q = V_f$.*

Proof. If $f \in \mathbb{A}_F$ and α is a root of f in L, then so is α^q. This follows since, if $g \in F[x]$ is the minimal polynomial of α, $g|f$ and $g(\alpha^q) = 0$ (α and α^q are conjugates since F is finite). Thus $V_f^q \subseteq V_f$. Since $x \to x^q$ is an automorphism of L over F, $V_f^q = V_f$.

If $V_f^q = V_f$ then we must show that $f \in F[x]$. The group H of automorphisms of L over F is the group generated by the automorphism $x \to x^q$. Thus V_f is invariant (as a set) under H. As the coefficients of f are symmetric functions of the elements of V_f, they are fixed by H, and therefore must be in F. Hence $f \in \mathbb{A}_F$. □

The preceding theorem gives the following alternative formulation of the bidecomposition problem for additive polynomials:

Let $F = GF(q)$ where $q, p, e \in \mathbb{N}$, p is prime, and $q = p^e$. Let K be an algebraic extension of F and let $V \subseteq K$ be a $\mathbb{Z}_p$ vector space of dimension ν over $\mathbb{Z}_p$ such that $V^q = V$. For a given σ with $1 \leq \sigma \leq \nu$, determine if there exists a σ dimensional subspace W of V such that $W^q = W$, and if so, give a basis for some predetermined number of them.

Since $V^q = V$, all the elements of V can be specified as the roots of a single additive polynomial $f \in \mathbb{A}_F$ of exponent ν. The found subspace W (if it exists) will be the kernel of a right composition factor $h \in \mathbb{A}_F$ of f of exponent σ.

3.3 Rational Decompositions of Additive Polynomials

We can now talk about decompositions of simple additive polynomials in general and their relationship to their kernels. For any $n, m \in \mathbb{N}$, let

$$\begin{aligned} \wp &= (r_m, r_{m-1}, \ldots, r_1) \\ &= (p^{\rho_m}, p^{\rho_{m-1}}, \ldots, p^{\rho_1}) \end{aligned}$$

be an ordered factorisation of n. Define

$$APDEC_{\wp}^F = \left\{ (f, (f_m, \ldots, f_1)) \in \mathbb{A}_F \times (\mathbb{A}_F)^m \;\middle|\; \begin{array}{l} f = f_m \circ \cdots \circ f_1 \\ \text{and } \deg f_i = r_i = p^{\rho_i} \end{array} \right\}.$$

Similarly, for simple additive polynomials, define

$$SAPDEC_{\wp}^F = \left\{ (f, (f_m, \ldots, f_1)) \in \mathbb{A}_F \times (\mathbb{A}_F)^m \;\middle|\; \begin{array}{l} f \text{ simple, } f = f_m \circ \cdots \circ f_1, \\ \text{and } \deg f_i = r_i = p^{\rho_i} \end{array} \right\}.$$

Obviously $SAPDEC_{\wp}^F \subseteq APDEC_{\wp}^F \subseteq DEC_{\wp}^F$.

Let $d_i = \prod_{1 \leq j \leq i} r_j$ and $\mathbb{V}$ be the set of all finite $\mathbb{Z}_p$ -vector spaces in F. Define

$$FLAGS_{\wp}^F = \left\{ (f, (V_m, \ldots, V_1)) \in \mathbb{A}_F \times \mathbb{V}^m \;\middle|\; \begin{array}{l} f \text{ simple, } V_m \text{ is the kernel of } f, \\ V_m \supseteq V_{m-1} \supseteq \cdots \supseteq V_1, \\ \dim V_i = d_i, \text{ for } 1 \leq i \leq m \end{array} \right\}.$$

The sequence $V_m \supseteq V_{m-1} \supseteq \cdots \supseteq V_1$ is called a *flag* of vector spaces associated with f.

Let $f \in \mathbb{A}_F$ be simple. For any $(f,(f_m,\ldots,f_1)) \in SAPDEC_{\wp}^F$ let $h_i = f_i \circ f_{i-1} \circ \cdots \circ f_1 \in \mathbb{A}_F$ and let V_i be the kernel of h_i. Then by theorems 3.1 and 3.3 $(f,(V_m,\ldots,V_1)) \in FLAGS_{\wp}^F$. Therefore, we define the map $\Gamma_{FL}^{SA} : SAPDEC_{\wp}^F \to FLAGS_{\wp}^F$ by $(f,(f_m,\ldots,f_1)) \mapsto (f,(V_m,\ldots,V_1))$.

Theorem 3.6. *Γ_{FL}^{SA} is a bijection between $SAPDEC_{\wp}^F$ and $FLAGS_{\wp}^F$.*

Proof. *Γ_{FL}^{SA} is injective since distinct additive polynomials have distinct kernels. If $(f,(V_m,V_{m-1},\ldots,V_1)) \in FLAGS_{\wp}^F$, then by theorem 3.3 the additive polynomial h_i with kernel V_i has a factor h_{i-1} with kernel V_{i-1}. Thus $h_i = f_i \circ h_{i-1}$ for some unique $f_i \in \mathbb{A}_F$ of degree $d_i/d_{i-1} = r_i$. Thus $(f,(f_m,\ldots,f_1)) \in SAPDEC_{\wp}^F$ and this map from $FLAGS_{\wp}^F$ to $SAPDEC_{\wp}^F$ is injective and is in fact the inverse of Γ_{FL}^{SA}. Thus Γ_{FL}^{SA} is a bijection.* □

3.4 The Number of Bidecompositions of a Polynomial

We will now compute the exact number of bidecompositions of a simple additive polynomial $f \in \mathbb{A}_F$ into two simple additive polynomials over its splitting field K. Assume f has exponent ν. The number of simple additive right composition factors of f in $K[x]$ of exponent σ is exactly the number of σ-dimensional subspaces of the kernel of f. This is calculated in the following well-known lemma.

Lemma 3.7. *The number of σ-dimensional subspaces of a ν-dimensional vector space V over $\mathbb{Z}_p$ is*

$$\mathcal{S}_{\sigma}^{\nu} = \frac{\prod\limits_{0 \le i < \sigma} (p^{\nu} - p^i)}{\prod\limits_{0 \le i < \sigma} (p^{\sigma} - p^i)}.$$

Proof. The number of linearly independent σ-tuples of vectors in V is

$$\prod_{0 \le i < \sigma} (p^{\nu} - p^i).$$

This is the number of all bases for all vector spaces of dimension σ. Each σ dimensional vector space has $\prod_{0 \le i < \sigma}(p^{\sigma} - p^i)$ bases. The lemma follows. □

The desired cardinality theorem now follows immediately.

Theorem 3.8. *Let $f \in \mathbb{A}_F$ be simple of exponent ν with splitting field K. The number of bidecompositions of f in $APDEC^K_{(p^{\nu-\sigma},p^\sigma)}$ is $\mathcal{S}^\nu_\sigma$.*

This theorem gives a super-polynomial lower bound for the number of decompositions of an arbitrary polynomial over an algebraic extension field.

Theorem 3.9. *For any even $\nu \in \mathbb{N}$, there exist monic polynomials $f \in F[x]$ of degree $n = p^\nu$ with splitting field K such that there are at least $n^{\lambda \log n}$ decompositions of f in $DEC^K_{(\sqrt{n},\sqrt{n})}$ where $\lambda = (6 \log p)^{-1}$.*

Proof. Assume $n = p^\nu$ where ν is even and let f be a simple additive polynomial of exponent ν. Then f has $\mathcal{S}^\nu_{\frac{\nu}{2}}$ decompositions in $DEC^K_{(\sqrt{n},\sqrt{n})}$.

$$\begin{aligned}
\mathcal{S}^\nu_{\frac{\nu}{2}} &= \frac{\prod_{0 \le i < \frac{\nu}{2}} (p^\nu - p^i)}{\prod_{0 \le i < \frac{\nu}{2}} (p^{\frac{\nu}{2}} - p^i)} \\
&\ge \frac{(p^{\nu-1})^{\frac{\nu}{2}}}{(p^{\frac{\nu}{2}})^{\frac{\nu}{2}}} \\
&= p^{\frac{\nu^2}{4} - \frac{\nu}{2}} \\
&\ge (p^\nu)^{\frac{\nu}{6}} \\
&= n^{\lambda \log n},
\end{aligned}$$

where $\lambda = (6 \log p)^{-1}$. $\square$

3.5 Complete Decompositions of Additive Polynomials

Let $n \in \mathbb{N}$ and let $\wp$ be a length m ordered factorisation of n. Complete decompositions of additive polynomials with ordered factorisation $\wp$ will be considered in a straightforward manner. Define the set $cAPDEC^F_\wp \subseteq cDEC^F_\wp$ to be the set of complete rational decompositions of additive polynomials with ordered factorisation $\wp$. By theorem 3.3 these will be decompositions into additive polynomials. Similarly, define the set $cSAPDEC^F_\wp \subseteq cAPDEC^F_\wp \subseteq cDEC^F_\wp$ to be the set of complete rational decompositions of simple additive polynomials with ordered factorisation $\wp$. The image of $cSAPDEC^F_\wp$ in $FLAGS^F_\wp$ will be called $cFLAGS^F_\wp$ and it too corresponds to the set of rational complete decompositions of simple additive polynomials. Members of $cFLAGS^F_\wp$ can also be characterised as those members of $FLAGS^F_\wp$ whose flags are maximal.

3.6 The Number of Complete Rational Normal Decompositions

In much the same way as we calculated the number of right composition factors of given exponent of a polynomial in theorem 3.7, we calculate the number of complete decompositions of a polynomial over an extension field. Let $f \in \mathbb{A}_F$ be simple with exponent ν and kernel V_f. The number of complete decompositions $\mathcal{F}^\nu$ of f over its splitting field K is equal to the number of maximal flags in V_f, and turns out to be dependent only on ν, not on f. As all subspaces of V_f are rational in K, each maximal flag will have ν subspaces and will have the form

$$V_f = V_\nu \supsetneq V_{\nu-1} \supsetneq \cdots \supsetneq V_1$$

where $\dim V_i = i$. The corresponding complete decompositions will be into exponent one, *p-linear*, composition factors.

Lemma 3.10. *The number of σ-dimensional subspaces of a ν-dimensional vector space V over $\mathbb{Z}_p$ which contain a given $(\sigma-1)$-dimensional vector space W is*

$$\mathcal{T}_\sigma^\nu = \frac{p^\nu - p^{\sigma-1}}{p^\sigma - p^{\sigma-1}}$$

Proof. There are $p^\nu - p^{\sigma-1}$ vectors of V which are linearly independent with W. A given σ-dimensional vector space containing W is generated by W plus any one of $p^\sigma - p^{\sigma-1}$ vectors. The lemma follows. □

The following lemma gives bounds for $\mathcal{F}^\nu$, and hence for the number of complete decompositions of f over K.

Lemma 3.11. *Let $f \in \mathbb{A}_F$ be simple of exponent ν with splitting field K. The maximum number $\mathcal{F}^\nu$ of distinct complete normal decompositions of f over K is bounded by*

$$p^{\frac{\nu^2}{2}} \leq \mathcal{F}^\nu \leq p^{\frac{\nu^2}{2}+\frac{3\nu}{2}}.$$

Proof. The fact that there are $\mathcal{F}^\nu$ distinct complete normal decompositions of f over K follows from the preceding discussion. We get the bounds as follows:

$$\begin{aligned}
\mathcal{F}^\nu &= \prod_{1\le i\le \nu} \mathcal{T}_i^\nu \\
&= \prod_{1\le i\le \nu} \frac{p^\nu - p^{i-1}}{p^i - p^{i-1}} \\
&\le \prod_{1\le i\le \nu} p^{\nu-i+1} \\
&\le p^{\frac{\nu^2}{2}+\frac{3\nu}{2}},
\end{aligned}$$

$$\begin{aligned}
\mathcal{F}^\nu &= \prod_{1\le i\le \nu} \mathcal{T}_i^\nu \\
&= \prod_{1\le i\le \nu} \frac{p^\nu - p^{i-1}}{p^i - p^{i-1}} \\
&\ge \prod_{1\le i\le \nu} p^{\nu-i} \\
&\ge p^{\frac{\nu^2}{2}}. \qquad \square
\end{aligned}$$

$\mathcal{F}^\nu$ is at least $n^{\mu \log n}$ where $\mu = (2 \log p)^{-1}$ and is super-polynomial in the degree n of f, and so there is a super-polynomial number of different complete normal decompositions of f over K. However, this does not guarantee that these decompositions are inequivalent in the sense that Ritt[1922] considered for the characteristic zero case. We now consider this question in the wild case.

As we saw in section 1.F, in the tame case there are two types of ambiguous decompositions. Recall that if $u \in F[x]$ and $m, r \in \mathbb{N}$, then $(x^m \cdot u^r) \circ x^r = x^r \circ (x^m \cdot u(x^r))$, an exponential ambiguity. If $x^m \cdot u^r$ and $x^m u(x^r)$ are indecomposable and additive, then since they are necessarily squarefree, r and m are at most one. In the case of additive polynomials therefore, exponential ambiguity is simply identity. The second kind of ambiguity in the tame case are trigonometric ambiguities – ambiguities arising from the commutative properties of the Chebyshev polynomials under composition. As we saw in theorem 1.13, the Chebyshev polynomial $T_{p^i} = x^{p^i}$, for $i \in \mathbb{N}$, in fields of characteristic p greater than two. In fields of characteristic $p = 2$, $T_{p^i} = 1$ if i is even and x if i is odd. Instead of restricting ourselves to

equivalence under these two types of ambiguities, we define the more general concept of a *permutation* ambiguity. Two complete normal decompositions are *permutation equivalent* if the composition factors of one are a permutation of the composition factors of the other. Trigonometric ambiguities are certainly encompassed in this definition. We now proceed to construct a class of polynomials which have a super-polynomial number (in their degrees) of permutation inequivalent decompositions over their splitting fields.

Theorem 3.12. *Let $p \in \mathbb{N}$ be prime, $\nu \in \mathbb{N}$ and $F = GF(p^\nu)$. Also, let K be an algebraic extension of F of degree p^ν over F. Then there exist simple additive polynomials $\hat{f} \in K[x]$ of exponent ν which have $\mathcal{F}^\nu \geq p^{\frac{\nu^2}{2}}$ pairwise permutation inequivalent complete normal decompositions in $cSAPDEC_*^K$.*

Proof. Let $(\theta_1, \ldots, \theta_\nu)$ be a basis for an algebraic extension F of $\mathbb{Z}_p$ of degree ν. Also, let $f = x^{p^\nu} - x \in F[x]$, and $\varepsilon \in \bar{F}$ (where $\bar{F}$ is an algebraic closure of F) be algebraic of degree p^ν over F. Consider the polynomial $\hat{f}$ with roots consisting of all elements of $K = F[\varepsilon]$ of the form εa for $a \in F$. The roots of $\hat{f}$ have a basis $(\varepsilon\theta_1, \ldots, \varepsilon\theta_\nu)$ over $\mathbb{Z}_p$. As in the construction of theorem 3.1, we now describe complete decompositions of f and $\hat{f}$ with respect to the bases $(\theta_1, \ldots, \theta_\nu)$ and $(\varepsilon\theta_1, \ldots, \varepsilon\theta_\nu)$. Let

$$\begin{aligned} \Psi_1 &= x^p - \theta_1^{p-1}x \in F[x], \qquad \text{and} \\ \hat{\Psi}_1 &= x^p - (\varepsilon\theta_1)^{p-1}x \in K[x]. \end{aligned}$$

For $i > 1$, define

$$\begin{aligned} \Psi_i &= (x^p - \Psi_{i-1}(\theta_i)^{p-1}x) \circ \Psi_{i-1} \in F[x], \qquad \text{and} \\ \hat{\Psi}_i &= (x^p - \hat{\Psi}_{i-1}(\varepsilon\theta_i)^{p-1}x) \circ \hat{\Psi}_{i-1} \in K[x]. \end{aligned}$$

Then

$$\begin{aligned} f = \Psi_\nu &= (x^p - \Psi_{\nu-1}(\theta_\nu)^{p-1}x) \circ \cdots \circ (x^p - \theta_1^{p-1}x), \qquad \text{and} \\ \hat{f} = \hat{\Psi}_\nu &= (x^p - \hat{\Psi}_{\nu-1}(\varepsilon\theta_\nu)^{p-1}x) \circ \cdots \circ (x^p - (\varepsilon\theta_1)^{p-1}x). \end{aligned}$$

Since, for $1 \leq i \leq \nu$,

$$\hat{\Psi}_i = \prod_{(a_1,\ldots,a_i)\in\mathbb{Z}_p^i} (x - \sum_{1\leq j\leq i} a_j\theta_j\varepsilon) \ ,$$

we find that

$$\begin{aligned}\hat{\Psi}_{i-1}(\varepsilon\theta_i) &= \prod_{(a_1,\ldots,a_{i-1})\in\mathbb{Z}_p^{i-1}} (\varepsilon\theta_i - \sum_{1\le j\le i-1} a_j\theta_j\varepsilon) \\ &= \varepsilon^{p^{i-1}} \prod_{(a_1,\ldots,a_{i-1})\in\mathbb{Z}_p^{i-1}} (\theta_i - \sum_{1\le j\le i-1} a_j\theta_j) \\ &= \varepsilon^{p^{i-1}}\Psi_{i-1}(\theta_i).\end{aligned}$$

Thus, in any decomposition of $\hat{f}$ into p-linear components in $K[x]$, for $1 \le i \le \nu$, the i^{th} composition factor has the form

$$x^p - a\varepsilon^{p^{i-1}(p-1)}x$$

for some $a \in F$. If any non-identity permutation of a decomposition was also a decomposition of $\hat{f}$, then

$$a\varepsilon^{p^{i-1}(p-1)} = b\varepsilon^{p^{j-1}(p-1)}$$

for some $1 \le i < j \le \nu$ and $a, b \in F$. But then ε would satisfy a polynomial in $F[x]$ of degree less than p^ν, giving a contradiction. It follows that for the class of polynomials just constructed there are $\mathcal{F}^\nu$ permutation inequivalent, complete normal decompositions. □

The above theorem gives a super-polynomial lower bound on the number of permutation inequivalent, complete normal decompositions possible for an arbitrary polynomial.

Theorem 3.13. *Let p be a prime number, $\nu \in \mathbb{N}$, and $n = p^\nu$. There exist fields K of algebraic degree at most $n \log n$ over $\mathbb{Z}_p$, and monic polynomials of degree n in $K[x]$ which have $n^{\mu \log n}$ decompositions in $cDEC_*^K$ which are inequivalent up to exponential and permutation ambiguities (where $\mu = (2\log p)^{-1}$).*

Proof. Let $f \in \mathbb{A}_F$ be simple of degree $n = p^\nu$ as constructed in theorem 3.11. By lemma 3.11 we know f has at least

$$p^{\frac{v^2}{2}} = n^{\mu \log n}$$

complete normal decompositions in $K[x]$ (where $\mu = (2\log p)^{-1}$), and these decompositions are inequivalent up to exponential and permutation ambiguities. The field K in theorem 3.11 has degree $\nu p^\nu = O(n \log n)$ over $\mathbb{Z}_p$. □

Additive polynomials are certainly not the only class of polynomials which potentially have a super-polynomial number (in their degrees) of inequivalent decompositions. For example, let $\mathcal{Q}$ be a set of additive polynomials which have a super-polynomial number of inequivalent decompositions in their degrees (such as that defined in theorem 3.11). Define a new set of polynomials

$$\mathcal{D} = \{g \circ f \circ g | f \in \mathcal{Q},\ g \in F[x],\ \deg f = \deg g = n\}.$$

Each $f \in \mathcal{D}$ has a super-polynomial number of decompositions in its degree and yet $\mathcal{D}$ is not a set of additive polynomials.

4 The Ring of Additive Polynomials

4.1 Basic Ring Structure

Ore[1933a] considers rings of polynomials $R_F \subseteq F[x]$ under the usual polynomial addition ($+$), and a (possibly non-commutative) multiplication ($\times$). The only further assumption he makes is the existence of a degree function $\delta : R_F \setminus \{0\} \to \mathbb{N}$ such that if $f, g \in R_F$ with $\delta(f) = r$ and $\delta(g) = s$, then $\delta(f \times g) = r + s$. In Ore[1933b] he applies this theory to the ring $\mathbb{A}_F$ of additive polynomials with composition as ring multiplication and exponent as the degree function. In this chapter, in sections A-D we present a summary of the theory of Ore as applied to additive polynomials. In section E we investigate the uniqueness properties of decompositions, and some properties of the indecomposable composition factors. We also strengthen a theorem of Ore[1933a] as applied to additive polynomials. In section F we use the relationships between decompositions developed in the previous sections to give an upper bound on the number of complete rational decompositions of an arbitrary additive polynomial. In chapter 5 we will then use the theory developed here to construct decomposition algorithms for additive polynomials.

Recall from chapter 3 that if F is a field of characteristic p then $f \in F[x]$ is additive if $f(x + y) = f(x) + f(y)$ for independent indeterminates x and y. We denote the set of all additive polynomials over F as $\mathbb{A}_F \subseteq F[x]$ and for $f \in \mathbb{A}_F$,

$$f = \sum_{0 \le i \le \nu} a_i x^{p^i}$$

with $a_i \in F$ for $0 \le i \le \nu$ and $a_\nu \neq 0$. The integer $\nu \ge 0$ is called the exponent of f and we write $\operatorname{expn} f = \nu$. It is easy to see that $\mathbb{A}_F$ is a ring without zero divisors. We will also show it has a right division algorithm (ie. if $f, g \in \mathbb{A}_F$, with $g \neq 0$, then there exists $Q, R \in \mathbb{A}_F$ such that $f = Q \circ g + R$ and $\operatorname{expn} R < \operatorname{expn} g$), and is therefore a left-Euclidean ring (the terminology is derived from the fact that the right division algorithm makes it a principal left ideal ring). Let $f, g \in \mathbb{A}_F$ with $g \neq 0$ and $\operatorname{expn} f = \nu$, and $\operatorname{expn} g = \rho$. Assume also that f and g have leading (high order) coefficients $a \in F$ and $b \in F$ respectively. If $\nu < \rho$ then division is trivial. If $\nu \ge \rho$ then with $f^{(\nu)} = f$, define

$$h^{(\nu)} = a b^{-p^{\nu-\rho}} x^{p^{\nu-\rho}} \in \mathbb{A}_F$$

and

$$f^{(\nu-1)} = f^{(\nu)} - h^{(\nu)} \circ g \in \mathbb{A}_F.$$

Then $f^{(\nu)} = h^{(\nu)} \circ g + f^{(\nu-1)}$ and $f^{(\nu-1)}$ has exponent less than that of $f^{(\nu)}$. Iterating this process we get

$$f = (h^{(\nu)} + h^{(\nu-1)} + \cdots + h^{(\rho)}) \circ g + f^{(\rho-1)}$$

and the exponent of $f^{(\rho-1)}$ is less than the exponent of g. This gives a right hand division algorithm for $\mathbb{A}_F$.

Let $f, g, h \in \mathbb{A}_F$. If $f = g \circ h$, then we write $h \phi f$, meaning h is a right composition factor of f. We will write $g = f \not\phi h$ meaning g is the compositional quotient after dividing f by h on the right (provided h does divide f on the right). This quotient is unique because of the existence of the division algorithm shown above (or by lemma 1.1). Finally, if $h \phi f - g$, then we write $f \equiv g \bmod h$. As an example, with $F = \mathbb{Z}_3$, let

$$\begin{aligned} f &= x^{27} + 2x^9 + x^3 + 2x, \\ g &= x^9 + x^3 + x. \end{aligned}$$

Then

$$\begin{aligned} f &= x^3 \circ g + x^9 + 2x \\ &= x^3 \circ g + x \circ g + 2x^3 + x \\ &= (x^3 + x) \circ g + (2x^3 + x). \end{aligned}$$

4.2 The Euclidean Scheme

From the existence of a right division algorithm for $\mathbb{A}_F$ follows the existence of a right Euclidean algorithm. Given $f_1, f_2 \in \mathbb{A}_F$, we proceed with the Euclidean scheme in the usual fashion (see van der Waerden [1970] pp. 55). Assume $\operatorname{expn} f_1 \geq \operatorname{expn} f_2$. At each stage $i > 2$, let f_i be the remainder of f_{i-2} divided on the right by f_{i-1}. We get the following sequence:

$$\begin{aligned} f_1 &= Q_1 \circ f_2 + f_3, \\ f_2 &= Q_2 \circ f_3 + f_4, \\ f_3 &= Q_2 \circ f_4 + f_5, \\ &\vdots \\ f_{n-2} &= Q_{n-2} \circ f_{n-1} + f_n, \\ f_{n-1} &= Q_{n-1} \circ f_n, \end{aligned}$$

where $Q_i, f_i \in \mathbb{A}_F$ and $\operatorname{expn} f_i < \operatorname{expn} f_{i-1}$. The number of steps n is at most the exponent of f_2. The polynomial $af_n \in \mathbb{A}_F$, where $a \in F$ is such that af_n is monic, is the greatest common (right compositional) divisor or *meet* of f_1 and f_2. We denote the meet $f_1 \sqcap f_2$. As an example, assume as before that $F = \mathbb{Z}_3$ and

$$\begin{aligned} f_1 &= x^{27} + 2x^9 + x^3 + 2x, \\ f_2 &= x^9 + x^3 + x. \end{aligned}$$

Following the Euclidean scheme,

$$\begin{aligned} f_1 &= (x^3 + x) \circ f_2 + (2x^3 + x), \\ f_2 &= (2x^3 + x) \circ (2x^3 + x), \\ f_3 &= 2x^3 + x. \end{aligned}$$

Normalising to make the meet monic,

$$\begin{aligned} f_1 \sqcap f_2 &= 2^{-1}(2x^3 + x) \\ &= x^3 + 2x. \end{aligned}$$

The existence of a Euclidean algorithm means $\mathbb{A}_F$ is a principal left ideal ring. Let f_1 and f_2 be two additive polynomials, and let (f_1) and (f_2) be the left ideals generated by them. The ideal $D = (f_1) + (f_2)$ consists of all sums of left multiples of f_1 with left multiples of f_2. Because $\mathbb{A}_F$ is principal, $D = (u)$ for some unique monic $u \in \mathbb{A}_F$ and this u is the meet of f_1 and f_2. The set $L = (f_1) \cap (f_2)$ is also an ideal and consists of all common left multiples of f_1 and f_2. Assume $f_1 f_2 \neq 0$. We must now show that $L \neq (0)$. Let $D = f_1 \sqcap f_2$. From the extended Euclidean scheme we know that there exist $A_1, A_2 \in \mathbb{A}_F$ such that $A_1 \circ f_1 + A_2 \circ f_2 = D$. If $f_2 = R_2 \circ D$ for $R_2 \in \mathbb{A}_F$, then $R_2 \circ A_1 \circ f_1 + R_2 \circ A_2 \circ f_2 = f_2$ and $R_2 \circ A_1 \circ f_1 = (x - R_2 \circ A_2) \circ f_2$. Thus f_1 and f_2 are both right factors of $R_2 \circ A_1 \circ f_1$, and since this is nonzero, $L \neq (0)$. The ring $\mathbb{A}_F$ is a principal left ideal ring, so $L = (h)$ for some unique monic $h \in F[x]$. This is the common left multiple of f_1 and f_2 of least exponent, which we will call the *join* of f_1 and f_2. We denote the join of f_1 and f_2 by $f_1 \sqcup f_2$. Some properties of the join are summarised in the following lemma.

Lemma 4.1. *Let* $f, g, h \in \mathbb{A}_F$.

(i) $f \sqcup g = g \sqcup f$,
(ii) $f \sqcup (g \sqcup h) = (f \sqcup g) \sqcup h$ *(we will often write* $f \sqcup g \sqcup h$*),*
(iii) $g \sqcup (f \circ g) = f \circ g$,
(iv) $(g \circ h) \sqcup (f \circ h) = (g \sqcup f) \circ h$,
(v) if $g \oint f$ *and* $h \oint f$ *then* $g \sqcup h \oint f$.

Proof. Let (f), (g), (h) be the left ideals generated by f, g, and h respectively.

(i) The polynomial $f \sqcup g$ is the unique monic generator of the ideal $(f) \cap (g) = (g) \cap (f)$, and as intersection is commutative, so is the join.
(ii) The polynomial $f \sqcup (g \sqcup h)$ is the unique monic generator of the ideal $(f) \cap ((g) \cap (h)) = ((f) \cap (g)) \cap (h) = (f) \cap (g) \cap (h)$ and by the associativity of intersection, join is associative.
(iii) Since $g \oint f \circ g$, $(f \circ g) \subseteq (g)$ and $(f \circ g) \cap (g) = (f \circ g)$.
(iv) The polynomial $(g \circ h) \sqcup (f \circ h)$ is the unique monic generator of the ideal $(f \circ h) \cap (g \circ h) = \{u \in \mathbb{A}_F \mid u = v \circ h \text{ and } v \in (f) \cap (g)\}$, since all common left multiples of $f \circ h$ and $g \circ h$ are also common multiples of f and g, composed with h. Since $(f) \cap (g)$ has generator $f \sqcup g$, the lemma follows.
(v) From the fact that $(g) \supseteq (f)$ and $(h) \supseteq (f)$ it follows that $(g) \cap (h) \supseteq (f)$ and therefore that $g \sqcup h \oint f$. □

The existence of a join does not give a construction for it. The standard commutative construction of the product divided by the greatest common divisor is not appropriate in a non-commutative ring. However, an extension to the Euclidean scheme will provide a more concrete representation of the join. We first require the following theorem.

Theorem 4.2. *Let* $f, g, h \in \mathbb{A}_F$. *If* $f \equiv g \bmod h$ *then*

$$f \sqcup h = a((g \sqcup h) \oint g) \circ f,$$

where $a \in F$ *is such that the join is monic.*

Proof. We know $g \sqcup h = u \circ g$ for some $u \in \mathbb{A}_F$. From the assumptions $f = g + Q \circ h$ for some $Q \in \mathbb{A}_F$ and $u \circ f = u \circ g + u \circ Q \circ h$. Since $h \oint u \circ g$

and $h \nmid u \circ Q \circ h$, we know $h \nmid u \circ f$. Because $f \nmid u \circ f$ as well, $h \sqcup f \nmid u \circ f$ by lemma 4.1 (v). We now show that in fact $h \sqcup f = a(u \circ f)$ where $a \in F$ is such that $a(u \circ f)$ is monic. Suppose $h \sqcup f = v \circ f$ for some $v \in \mathbb{A}_F$. Then $h \sqcup f = v \circ f = v \circ g + v \circ Q \circ h$ and since $h \nmid v \circ f$ and $h \nmid v \circ Q \circ h$, it follows that $h \nmid v \circ g$ as well. We know $g \nmid v \circ g$, so $g \sqcup h \nmid v \circ g$. Since $g \sqcup h = u \circ g$, $\operatorname{expn} v \geq \operatorname{expn} u$. Therefore $h \sqcup f = a(u \circ f)$. By definition $u = (g \sqcup h) \not\phi g$, so $h \sqcup f = a((g \sqcup h) \not\phi g) \circ f$. $\square$

The join of f_1 and f_2 can now be written as follows.

Theorem 4.3.

$$f_1 \sqcup f_2 = b(\cdots (f_{n-1} \not\phi f_n) \circ f_{n-2}) \not\phi f_{n-1}) \circ \cdots \circ f_3) \not\phi f_4) \circ f_2) \not\phi f_3) \circ f_1$$

for some $b \in F$ chosen to make the join monic (the alternation of $\circ$ and $\not\phi$ is similar to the alternation of $+$ and $\cdot$ in Horner's rule, and the difference between successive indices (from left to right) is $+1, -2, +1, -2, +1, \ldots$ for each of the $2n-1$ terms).

Proof. In the Euclidean scheme, $f_i \bmod f_{i+2} \bmod f_{i+1}$ for $1 \leq i \leq n-1$ (with $f_{n+1} = 0$), where n is the length of the sequence of f_i's in the Euclidean scheme. Also note that $f_n \nmid f_{n-1}$. From theorem 4.2 this implies that

$$f_i \sqcup f_{i+1} = a((f_{i+1} \sqcup f_{i+2}) \not\phi f_{i+2}) \circ f_i.$$

for some $a \in F$. We proceed by induction on n.
If $n = 2$ then $f_1 \sqcup f_2 = f_1$ and the theorem holds immediately.
Now assume that the theorem holds for Euclidean schemes of length less than n. If the Euclidean scheme has length n, then

$$f_1 \sqcup f_2 = a_1([f_2 \sqcup f_3] \not\phi f_3) \circ f_1,$$

and by induction,

$$\begin{aligned} f_1 \sqcup f_2 &= a_1([a_2(\cdots (f_{n-1} \not\phi f_n) \circ f_{n-2}) \not\phi \cdots \not\phi f_5) \circ f_3) \not\phi f_4) \circ f_2] \not\phi f_3) \circ f_1 \\ &= b(\cdots (f_{n-1} \not\phi f_n) \circ f_{n-2}) \not\phi \cdots \not\phi f_5) \circ f_3) \not\phi f_4) \circ f_2) \not\phi f_3) \circ f_1 \end{aligned}$$

for appropriate $a_1, a_2, b \in F$, and the theorem follows. $\square$

Theorem 4.3 also allows us to calculate the exponent of the join.

Theorem 4.4. $\operatorname{expn}(f_1 \sqcup f_2) = \operatorname{expn} f_1 + \operatorname{expn} f_2 - \operatorname{expn}(f_1 \sqcap f_2)$

Proof. Using the simple fact that $\operatorname{expn} f \circ g = \operatorname{expn} f + \operatorname{expn} g$ and $\operatorname{expn} f \not\circ g = \operatorname{expn} f - \operatorname{expn} g$, for $f, g \in \mathbb{A}_F$, a quick examination of the formula for join given in theorem 4.3 reveals that

$$\begin{aligned} \operatorname{expn} f_1 \sqcup f_2 &= \operatorname{expn} f_1 + \operatorname{expn} f_2 - \operatorname{expn} f_n \\ &= \operatorname{expn} f_1 + \operatorname{expn} f_2 - \operatorname{expn}(f_1 \sqcap f_2) \end{aligned}$$

and the theorem is proved. □

Continuing with the previous example,

$$\begin{aligned} f_1 \sqcup f_2 &= a((f_2 \not\circ f_3) \circ f_1) \\ &= a(((2x^3 + x) \circ (2x^3 + x)) \not\circ (2x^3 + x)) \circ f_1 \\ &= a(2x^3 + x) \circ (x^{27} + 2x^9 + x^3 + 2x) \\ &= a(2x^{81} + 2x^{27} + x^9 + 2x^3 + 2x) \\ &= x^{81} + x^{27} + 2x^9 + x^3 + x. \end{aligned}$$

For verification we check that indeed

$$\begin{aligned} x^{81} + x^{27} + 2x^9 + x^3 + x &= (x^9 + x) \circ f_2 \\ &= (x^3 + 2x) \circ f_1. \end{aligned}$$

If $f, g, h \in \mathbb{A}_F$ with $g \neq 0$ and $f = g \circ h$, then h is a multiplicative factor as well as a right composition factor of f. Thus, if

$$f = Q \circ g + R$$

where $Q, R \in \mathbb{A}_F$ and $\operatorname{expn} R < \operatorname{expn} g$, then

$$\begin{aligned} f - R &= Q \circ g \\ &= Q'g, \end{aligned}$$

where $Q' = (f - R)/g \in F[x]$. Therefore $f = Q'g + R$ and usual multiplicative division in $F[x]$ yields the same remainder as compositional division in $\mathbb{A}_F$. This means that the right-Euclidean algorithm for $\mathbb{A}_F$ just described generates the same sequence of f_i's as the usual multiplicative Euclidean algorithm (though obviously a different sequence of Q_i's) and we have the following theorem.

Theorem 4.5. *If $f_1, f_2 \in \mathbb{A}_F$, then $f_1 \sqcap f_2$ is equal to the usual multiplicative greatest common divisor of f_1 and f_2.*

We can speak of f_1 and f_2 in $\mathbb{A}_F$ as being *composition-coprime* if $f_1 \sqcap f_2 = x$, and this is equivalent to saying that the usual, multiplicative, greatest common divisor of f_1 and f_2 is x.

4.3 The Structure of the Set of Decompositions

The set of all distinct complete rational normal decompositions of a given additive polynomial has a very strong internal structure. Ore[1933a] develops this structure in the general context of non-commutative left-Euclidean polynomial rings.

The central concept of Ore's theory is that of *transformation*. Let $f, g \in \mathbb{A}_F$ be monic. The monic polynomial

$$g \triangleright f = (g \sqcup f) \oint g \ \in \mathbb{A}_F$$

is called the transformation of f by g. By theorem 4.4, we determine that

$$\begin{aligned} \operatorname{expn}(g \triangleright f) &= \operatorname{expn}(g \sqcup f) - \operatorname{expn} g \\ &= \operatorname{expn} g + \operatorname{expn} f - \operatorname{expn}(g \sqcap f) - \operatorname{expn} g \\ &= \operatorname{expn} f - \operatorname{expn}(g \sqcap f). \end{aligned}$$

Obviously, if f and g are composition-coprime then $\operatorname{expn}(g \triangleright f) = \operatorname{expn} f$ (though $g \triangleright f$ certainly does not have to equal f).

The properties of transformation will be developed in the following few theorems. There does not seem to be an easy technique relating these properties to the familiar multiplicative identities, say over the integers. Once might liken meet to integer greatest common divisor (gcd) and join to least common multiple (lcm). In this case transformation becomes lcm divided by gcd. But this is also a commutative construction, which is not the case for transformation in the additive polynomials.

Theorem 4.6. *Let $f, g, h \in \mathbb{A}_F$ be monic. If $f \eqq g \bmod h$ then $f \triangleright h = g \triangleright h$.*

Proof. By theorem 4.2, $f \sqcup h = ((g \sqcup h) \oint g) \circ f$. Dividing both sides on the right by f, we get $(f \sqcup h) \oint f = (g \sqcup h) \oint g$ (the multiplying constant $a \in F$ from theorem 4.2 is one since f, g and h are assumed to be monic). Directly, we have that $f \triangleright h = g \triangleright h$. $\square$

Theorem 4.7. *Let $f, g, h \in \mathbb{A}_F$ be monic. If $h \mathbin{\phi} f \circ g$ then*

(i) $(g \triangleright h) \mathbin{\phi} f$, and
(ii) if f is indecomposable, $g \sqcap h = x$, and $h \neq x$, then $g \triangleright h = f$.

Proof.

(i) The polynomials g and h are both right factors of $f \circ g$, so there exists a $u \in \mathbb{A}_F$ such that $f \circ g = u \circ (g \sqcup h)$. Thus

$$\begin{aligned} f &= (u \circ (g \sqcup h)) \mathbin{\phi} g \\ &= u \circ (g \triangleright h). \end{aligned}$$

(ii) As f is indecomposable and $g \sqcap h = x$, we know $\operatorname{expn}(g \triangleright h) = \operatorname{expn} h$. From (i), $(g \triangleright h) \mathbin{\phi} f$ and since $\operatorname{expn} h = \operatorname{expn}(g \triangleright h) > 0$ and f is indecomposable, $(g \triangleright h) = f$. □

Two monic additive polynomials $f, g \in \mathbb{A}_F$ are said to be *similar* if there exists a $u \in \mathbb{A}_F$ composition-coprime with g such that $f = u \triangleright g$. To denote similarity we write $f \sim g$. Note that if f and g are similar then $\operatorname{expn} f = \operatorname{expn} g$. We will show that similarity is an equivalence relation. First, we must prove a preliminary lemma.

Lemma 4.8. *Let $f, g, h \in \mathbb{A}_F$ be monic. Then $(g \circ h) \triangleright f = g \triangleright (h \triangleright f)$.*

Proof.

$$\begin{aligned} (g \circ h) \triangleright f &= ((g \circ h) \sqcup f) \mathbin{\phi} (g \circ h) \\ &= ((g \circ h) \sqcup h \sqcup f) \mathbin{\phi} (g \circ h) \\ &= ((g \circ h) \sqcup (h \sqcup f)) \mathbin{\phi} h) \mathbin{\phi} g \\ &= (g \sqcup ((h \sqcup f) \mathbin{\phi} h)) \mathbin{\phi} g \\ &= g \triangleright (h \triangleright f). \end{aligned}$$ □

Theorem 4.9. *Similarity is an equivalence relation.*

Proof. Let $f, g, h \in \mathbb{A}_F$ be monic.

(i) Similarity is reflexive since $x \triangleright f = f$.

(ii) Assume $f \sim g$, so that $f = u \triangleright g$ for some $u \in \mathbb{A}_F$ such that $u \sqcap g = x$. As u and g are composition-coprime, there exist $Q, v \in \mathbb{A}_F$ such that

$$v \circ u + Q \circ g = x.$$

Therefore $v \circ u \equiv x \bmod g$. We have

$$\begin{aligned} g = x \triangleright g &= (v \circ u) \triangleright g && \text{by theorem 4.6} \\ &= v \triangleright (u \triangleright g) && \text{by lemma 4.8} \\ &= v \triangleright f, \end{aligned}$$

and $g \sim f$, so similarity is symmetric.

(iii) Assume $f \sim g$ and $g \sim h$. Then there exist $u, v \in \mathbb{A}_F$ such that $u \sqcap g = x$, $f = u \triangleright g$, $v \sqcap h = x$, and $g = v \triangleright h$. By lemma 4.8,

$$\begin{aligned} f &= u \triangleright g \\ &= u \triangleright (v \triangleright h) \\ &= (u \circ v) \triangleright h. \end{aligned}$$

Because h and f have the same exponent, $(u \circ v) \sqcap h = x$ and $h \sim f$. Thus similarity is transitive.

By (i), (ii), and (iii) above, similarity is an equivalence relation. □

An interesting case is that of the additive polynomial x^p, which has the following property.

Lemma 4.10. *The only additive polynomial similar to $x^p \in \mathbb{A}_F$ is x^p.*

Proof. Let $u \in \mathbb{A}_F$ be monic and composition-coprime with x^p. Thus, u is simple (u is monic and $u(0) = 0$). Since $u \sqcup x^p = w \circ x^p$ for some $w \in \mathbb{A}_F$, $u \sqcup x^p$ is not simple. We also know that $u \sqcup x^p = v \circ u$ for some $v = x^p + ax \in \mathbb{A}_F$ for some $a \in F$. As u is simple and $v \circ u$ is not simple, $v = x^p$. Therefore $u \sqcup x^p = x^p \circ u$ and $u \triangleright x^p = x^p$. □

A further property of transformation is that the transformation of a join is simply the transformation of its components.

Theorem 4.11. *Let $f, g, h \in \mathbb{A}_F$ be monic. Then $h \triangleright (f \sqcup g) = (h \triangleright f) \sqcup (h \triangleright g)$.*

Proof. We know

$$\begin{aligned}(h \triangleright (f \sqcup g)) \circ h &= ((h \sqcup (f \sqcup g)) \not\phi\ h) \circ h \\ &= (h \sqcup (f \sqcup g)) \\ &= (h \sqcup f) \sqcup (h \sqcup g) \\ &= (((h \sqcup f) \not\phi\ h) \sqcup ((h \sqcup g) \not\phi\ h)) \circ h.\end{aligned}$$

Dividing on the right by h we get

$$h \triangleright (f \sqcup g) = (h \triangleright f) \sqcup (h \triangleright g). \qquad \square$$

Transformation will later be used to characterise the different decompositions of a given additive polynomial. It will be useful to know the effect of transformation on a composition of additive polynomials.

Theorem 4.12. *Let $f, g, h \in \mathbb{A}_F$ be monic. Then $h \triangleright (f \circ g) = ((g \triangleright h) \triangleright f) \circ (h \triangleright g)$.*

Proof. We know that

$$\begin{aligned}h \triangleright (f \circ g) &= h \triangleright ((f \circ g) \sqcup g) \\ &= (h \triangleright (f \circ g)) \sqcup (h \triangleright g) \qquad \text{(by theorem 4.11)} \\ &= Q \circ (h \triangleright g)\end{aligned}$$

for some $Q \in \mathbb{A}_F$. This implies $Q \circ (h \sqcup g) = h \sqcup (f \circ g)$ and

$$\begin{aligned}Q \circ (g \triangleright h) &= (h \sqcup (f \circ g)) \not\phi\ g \\ &= (g \sqcup (h \sqcup (f \circ g))) \not\phi\ g \\ &= g \triangleright (h \sqcup (f \circ g)) \\ &= (g \triangleright h) \sqcup (g \triangleright (f \circ g)) \\ &= (g \triangleright h) \sqcup ((g \sqcup (f \circ g)) \not\phi\ g) \\ &= (g \triangleright h) \sqcup f.\end{aligned}$$

Therefore, $Q = (g \triangleright h) \triangleright f$ and the theorem follows. $\square$

This theorem can be easily extended to consider the transformation of a composition of many polynomials.

Theorem 4.13. *Let $f \in \mathbb{A}_F$ be monic. Assume $f = f_m \circ f_{m-1} \circ \cdots \circ f_1$ where $f_i \in \mathbb{A}_F$ are monic for $1 \leq i \leq m$. Let $h \in \mathbb{A}_F$ be monic and composition-coprime with f. If $h_i \in \mathbb{A}_F$ is defined by*

$$h_i = \begin{cases} (f_{i-1} \circ f_{i-2} \circ \cdots \circ f_1) \triangleright h & \text{for } i > 1, \\ h & \text{for } i = 1, \end{cases}$$

for $1 \leq i \leq m$ then

$$h \triangleright f = \bar{f}_m \circ \bar{f}_{m-1} \circ \cdots \circ \bar{f}_1,$$

where $\bar{f}_i = h_i \triangleright f_i$.

Proof. We proceed by induction on m. If $m = 1$ then $h \triangleright f_1 = \bar{f}_1$. Assume the theorem is true if the number of factors is less than m and that $m > 1$. From theorem 4.12,

$$\begin{aligned} h \triangleright f &= h \triangleright ((f_m \circ f_{m-1} \cdots \circ f_2) \circ f_1) \\ &= ((f_1 \triangleright h) \triangleright (f_m \circ \cdots \circ f_2)) \circ (h \triangleright f_1). \end{aligned}$$

Since h and f are composition-coprime, $\operatorname{expn} h \triangleright f = \operatorname{expn} f$. Therefore, by computing the exponents of each side of the above equation, we have

$$\operatorname{expn}(f_m \circ \cdots \circ f_2) = \operatorname{expn}((f_1 \triangleright h) \triangleright (f_m \circ \cdots \circ f_2)),$$

and $(f_1 \triangleright h)$ and $f_m \circ \cdots \circ f_2$ must be composition-coprime. By induction,

$$(f_1 \triangleright h) \triangleright (f_m \circ \cdots f_2) = \bar{f}_m \circ \bar{f}_{m-1} \circ \cdots \circ \bar{f}_2$$

with $\bar{f}_i = \bar{h}_i \triangleright f_i$ for $2 \leq i \leq m$ where $\bar{h}_i$ is defined by

$$\begin{aligned} \bar{h}_i &= \begin{cases} (f_{i-1} \circ f_{i-2} \circ \cdots \circ f_2) \triangleright (f_1 \triangleright h) & \text{for } i > 2 \\ f_1 \triangleright h & \text{for } i = 2 \end{cases} \\ &= (f_{i-1} \circ \cdots \circ f_2) \triangleright h \qquad \text{(by lemma 4.8)}, \end{aligned}$$

and the theorem follows. □

The above theorems consider the transformations of arbitrary decompositions. What are the effects of transformation on complete decompositions? We first need to know the relationship between the decompositions of similar additive polynomials.

Theorem 4.14. *If $f, g \in \mathbb{A}_F$, $f \sim g$ and f is indecomposable, then g is indecomposable.*

Proof. Assume $f = u \triangleright g$ for some $u \in \mathbb{A}_F$ composition-coprime with g. Suppose that $g = g_2 \circ g_1$, where $\operatorname{expn} g_2 > 0$ and $\operatorname{expn} g_1 > 0$ (so g is decomposable). By theorem 4.12, $f = ((g_1 \triangleright u) \triangleright g_2) \circ (u \triangleright g_1)$. The polynomials u and g_1 are composition-coprime because u and g are composition-coprime and $g_1 \nmid g$. It follows that $u \triangleright g_1 \sim g_1$ and $\operatorname{expn} u \triangleright g_1 = \operatorname{expn} g_1$. Therefore $\operatorname{expn}((g_1 \triangleright u) \triangleright g_2) = \operatorname{expn} g_2$ and f is decomposable, a contradiction. Therefore g is indecomposable. □

From 4.13 and 4.14 we immediately get the following theorem.

Theorem 4.15. *If $(f, (f_m, \ldots, f_1)) \in cAPDEC_*^F$ and $g \sim f$ (say $g = u \triangleright f$), then there exists $(g, (g_m, \ldots, g_1)) \in cAPDEC_*^F$ where $g_i \sim f_i$ for $1 \leq i \leq m$ (specifically, $g_1 = u \triangleright f_1$ for some $u \in \mathbb{A}_F$ and $g_i = ((f_{i-1} \circ \cdots \circ f_1) \triangleright u) \triangleright f_i$ for $2 \leq i \leq m$).*

Proof. By theorem 4.13 we transform the composition, giving a decomposition of g. The fact that this is a complete decomposition follows from 4.14. □

Transformation and similarity can be used to completely characterise the relationship between decompositions. Let $f, g \in \mathbb{A}_F$ be monic. If there exists a monic $\bar{f} \in \mathbb{A}_F$ such that $\bar{f} \sim f$ and $f = g \triangleright \bar{f}$, we say f and g are *transmutable* or that they *transmute*. The additive polynomial $\bar{f}$ is called a transmutation of f by g. In this case,

$$\begin{aligned} f \circ g &= (g \triangleright \bar{f}) \circ g \\ &= ((g \sqcup \bar{f}) \oblong g) \circ g \\ &= g \sqcup \bar{f} \\ &= ((\bar{f} \sqcup g) \oblong \bar{f}) \circ \bar{f} \\ &= (\bar{f} \triangleright g) \circ \bar{f} \\ &= \bar{g} \circ \bar{f} \end{aligned}$$

where $\bar{g} = \bar{f} \triangleright g \in \mathbb{A}_F$. Because $f \sim \bar{f}$, f and $\bar{f}$ have the same exponent and

so $\bar{g}$ and g also have the same exponent. We know

$$\begin{aligned}\operatorname{expn}(\bar{f} \sqcup g) &= \operatorname{expn} \bar{f} + \operatorname{expn} g - \operatorname{expn}(\bar{f} \sqcap g) \\ &= \operatorname{expn}(f \circ g) \\ &= \operatorname{expn}(\bar{f} \circ g) \\ &= \operatorname{expn} \bar{f} + \operatorname{expn} g.\end{aligned}$$

Thus $\operatorname{expn} \bar{f} \sqcap g = 0$ and $\bar{g} \sim g$.
There is no reason why there cannot exist an $\tilde{f} \in \mathbb{A}_F$ such that $\tilde{f} \sim f$, $\tilde{f} \neq \bar{f}$ and $f = g \triangleright \tilde{f}$. The transmutation of f by g is not unique. Consider the following example over an arbitrary field F of characteristic p.

$$\begin{aligned} f &= x^p + ax \qquad a \in F \\ g &= x^p + bx \qquad b \in F \end{aligned}$$

Then $f \circ g = x^{p^2} + (a + b^p)x^p + abx$. Assume $f \circ g = \bar{g} \circ \bar{f}$ where

$$\begin{aligned} \bar{f} &= x^p + \bar{a}x \qquad \bar{a} \in F \\ \bar{g} &= x^p + \bar{b}x \qquad \bar{b} \in F \end{aligned}$$

This implies $\bar{b} + \bar{a}^p = a + b^p$ and $ab = \bar{a}\bar{b}$. Thus

$$\begin{aligned} 0 &= ab - \bar{a}\bar{b} \\ &= ab - \bar{a}(-\bar{a}^p + a + b^p) \\ &= ab + \bar{a}^{p+1} - a\bar{a} - b^p\bar{a} \\ &= a(b - \bar{a}) - \bar{a}(b - \bar{a})^p \\ &= (b - \bar{a})(a - \bar{a}(b - \bar{a})^{p-1}), \end{aligned}$$

and either $f = \bar{g}$ and $\bar{f} = g$, or $\bar{a}$ is a root of $\varphi = a - x(b - x)^{p-1} \in F[x]$ ($\bar{g}$ is uniquely determined as $\bar{g} = (f \circ g) \oint \bar{f}$). Noting that

$$\begin{aligned} f &= (\bar{g} \circ \bar{f}) \oint g \\ &= (g \sqcup (\bar{g} \circ \bar{f})) \oint g \qquad\qquad \text{since } g \oint \bar{g} \circ \bar{f} \\ &= g \triangleright (\bar{g} \circ \bar{f}) \\ &= g \triangleright ((\bar{g} \circ \bar{f}) \sqcup \bar{f}) \\ &= g \triangleright (\bar{g} \circ \bar{f}) \sqcup (g \triangleright \bar{f}) \\ &= f \sqcup (g \triangleright \bar{f}), \end{aligned}$$

and $\operatorname{expn} f = \operatorname{expn} g \triangleright \bar{f} = 1$, it follows that $f = g \triangleright \bar{f}$, so $f \sim \bar{f}$ and the transmutation of f by g is $\bar{f}$. Since the argument can be reversed, it implies that the polynomial f can transmute by g in up to p different ways, depending upon the roots of φ in F.

A point worth noting is that x^p does not transmute by x^p. By lemma 4.10, the only polynomial similar to x^p is x^p. If x^p did transmute by x^p, then $x^p = x^p \triangleright x^p = (x^p \sqcup x^p) \not\phi\ x^p = x$, a contradiction.

The set of all complete decompositions of $f \in \mathbb{A}_F$ can be given structure using transmutation and similarity. Let $(f, (f_m, f_{m-1}, \ldots, f_1)) \in cAPDEC_*^F$. If f_i and $f_{i-1} \circ f_{i-2} \circ \cdots \circ f_\ell$ transmute for some $i, \ell \in \mathbb{N}$ with $m \geq i > \ell \geq 1$ then we get another complete decomposition of f. As in theorem 4.13, this is

$$(f, (f_m, f_{m-1}, \ldots, f_{i+1}, \bar{f}_{i-1}, \ldots, \bar{f}_\ell, \bar{f}_i, f_{\ell-1}, \ldots, f_1)) \in cAPDEC_*^F.$$

where $\bar{f}_j \sim f_j$ for $\ell \leq j \leq i$. We say these two decompositions are *single-transmutation equivalent*. Letting $(f, (f_m^{(0)}, \ldots, f_1^{(0)})) \in cAPDEC_*^F$, if there is a sequence

$$\begin{gathered}(f_m^{(0)}, \ldots, f_1^{(0)}) \\ (f_m^{(1)}, \ldots, f_1^{(1)}) \\ \vdots \\ (f_m^{(t)}, \ldots, f_1^{(t)})\end{gathered}$$

where $(f, (f_m^{(i)}, \ldots, f_1^{(i)})) \in cAPDEC_*^F$ for $1 \leq i \leq t$, and $(f_m^{(i)}, \ldots, f_1^{(i)})$ and $(f_m^{(i+1)}, \ldots, f_1^{(i+1)})$ are single-transmutation equivalent for $1 \leq i < t$, we say that $f_m^{(0)}, \ldots, f_1^{(0)}$ and $f_m^{(t)}, \ldots, f_1^{(t)}$ are *transmutation equivalent*. Transmutation equivalence is the reflexive transitive closure of single-transmutation equivalence.

Theorem 4.16. *All complete rational normal decompositions of a monic $f \in \mathbb{A}_F$ are transmutation equivalent.*

Proof. Let $(f, (f_m, \ldots, f_1)) = (f, (f_m^{(0)}, \ldots, f_1^{(0)}))$ and $(f, (g_r, \ldots, g_1))$ for $r, m \in \mathbb{N}$ be complete rational normal decompositions of f. We prove the theorem by induction on m. If $m = 1$ then f is indecomposable and $f_1 = g_1$, so the statement is true.

Assume the theorem is true for complete decompositions of length less than m. Let $k \in \mathbb{N}$ be the smallest number such that $g_1 \nmid (f_k \circ f_{k-1} \circ \cdots \circ f_1)$. If $k = 1$ then $f_1 = g_1$ (they are both indecomposable), and by induction $(f \notin g_1, (f_m, \ldots, f_2))$ and $(f \notin g_1, (g_r, \ldots, g_2)) \in cAPDEC_*^F$ are transmutation equivalent. Therefore $(f, (f_m, \ldots, f_1))$ and $(f, (g_r, \ldots, g_1))$ are transmutation equivalent.

If $k > 1$ then $f_{k-1} \circ f_{k-2} \circ \cdots \circ f_1$ and g_1 are composition-coprime. By theorem 4.7(ii),

$$f_k = (f_{k-1} \circ f_{k-2} \circ \cdots \circ f_1) \triangleright g_1,$$

$f_k \sim g_1$, and f_k and $(f_{k-1} \circ \cdots \circ f_1)$ are transmutable. Therefore

$$\begin{aligned} f_k \circ f_{k-1} \circ \cdots \circ f_1 &= (g_1 \triangleright (f_{k-1} \circ \cdots \circ f_1)) \circ g_1 \\ &= \bar{f}_{k-1} \circ \bar{f}_{k-2} \circ \cdots \circ \bar{f}_1 \circ g_1 \end{aligned}$$

by theorem 4.13, where $f_i \sim \bar{f}_i$ for $1 \leq i \leq k-1$. Thus

$$(f, (f_m, f_{m-1}, \ldots, f_{k+1}, \bar{f}_{k-1}, \ldots, \bar{f}_1, g_1))$$

and $(f, (f_m, \ldots, f_1))$ are single-transmutation equivalent. Also, by the inductive hypothesis, $(f \notin g_1, (f_m, f_{m-1}, \ldots, f_{k+1}, \bar{f}_{k-1}, \ldots, \bar{f}_1))$ and $(f \notin g_1, (g_r, \ldots, g_2))$ are transmutation equivalent. Therefore $(f, (f_m, \ldots, f_1))$ and $(f, (g_r, \ldots, g_1))$ are transmutation equivalent and the theorem follows. □

Any two single-transmutation equivalent decompositions have the same number of indecomposable factors in any complete decomposition, and these factors are similar in pairs. Since similarity is transitive, we immediately get the following corollary.

Corollary 4.17. *Any two complete decompositions of $f \in \mathbb{A}_F$ have the same number of factors and if $(f, (f_m, f_{m-1}, \ldots, f_1))$, $(f, (g_m, g_{m-1}, \ldots, g_1)) \in cAPDEC_*^F$ for some $m > 0$, there exists a permutation σ of $\{1, \ldots, m\}$ such that $g_i \sim f_{\sigma_i}$ for $1 \leq i \leq m$.*

4.4 Completely Reducible Additive Polynomials

A monic additive polynomial is said to be *completely reducible* if it is the join of a set of indecomposable additive polynomials. Completely reducible additive polynomials have a number of nice properties which we will examine mathematically and algorithmically.

Lemma 4.18. *A completely reducible polynomial $f \in \mathbb{A}_F$ can be represented in the form*

$$f = h_r \sqcup h_{r-1} \sqcup \cdots \sqcup h_1$$

where, for $1 \leq i \leq r$, h_i is indecomposable and no one of the h_i's is a right composition factor of the join of the others. This is called an indecomposable basis of f.

Proof. Let $f \in \mathbb{A}_F$ be completely reducible and let $u_1, u_2, \ldots, u_m \in \mathbb{A}_F$ be the indecomposable right factors of f. We know that f is the join of these right factors by the definition of completely reducible, and that there is a finite number of them since they are all multiplicative divisors of f. Consider the following method for determining an indecomposable basis for f.

```
1) Let T := ∅
2) Let g^(0) := x
3) For i from 1 to m
   3.1) if u_i ⊓ g^(i−1) = x then
            3.1.1) let g^(i) := g^(i−1) ⊔ u_i
            3.1.2) let T := T ∪ {u_i}
        else
            3.1.3) let g^(i) := g^(i−1)
   3.2) if g^(i) = f, then quit, returning T
```

At step 3.1, we know that if $u_i \sqcap g^{(i-1)} \neq x$ then $u_i \nmid g^{(i-1)}$ for $i \geq 1$ because u_i is indecomposable. In this case it will not change the join $g^{(i-1)}$ and is redundant. Because f is the join of all its indecomposable right factors, $g^{(k)} = f$ for some $k \leq m$. From the construction, the exponent of the join of the polynomials in T is the sum of the exponents of these polynomials. By theorem 4.4, therefore, any one polynomial in T is composition-coprime with the join of the others in T. $\square$

Note that we can choose any indecomposable right factor u_1 we want in the above procedure.

A polynomial $f \in \mathbb{A}_F$ is said to be *completely transmutable* if in any complete decomposition, any two adjacent indecomposable factors are transmutable.

Theorem 4.19. *An additive polynomial is completely reducible if and only if it is completely transmutable.*

Proof. We first show that if $f \in \mathbb{A}_F$ is completely reducible then it is completely transmutable. We proceed by induction on the number of indecomposable factors in a complete decomposition of f. Assume $f = g_1 \in \mathbb{A}_F$, where g_1 is indecomposable. Then f is completely transmutable. Now, assume the statement is true if f has less than m indecomposable factors in any complete decomposition. Let $f = g_m \circ g_{m-1} \circ \cdots \circ g_1 = \bar{g} \circ g_1$ where $g_i \in \mathbb{A}_F$ are indecomposable for $1 \leq i \leq m$ and $m > 2$, and $\bar{g} = f \oint g_1 \in \mathbb{A}_F$. As f is completely reducible, it has an indecomposable basis $\{g_1, h_2, h_3, \ldots, h_\ell\}$ with $h_i \in \mathbb{A}_F$ indecomposable for $2 \leq i \leq \ell$. We get

$$\begin{aligned}\bar{g} &= ((h_\ell \sqcup \cdots \sqcup h_2) \sqcup g_1) \oint g_1 \\ &= g_1 \triangleright (h_\ell \sqcup \cdots \sqcup h_2) \\ &= (g_1 \triangleright h_\ell) \sqcup (g_1 \triangleright h_{\ell-1}) \sqcup \cdots \sqcup (g_1 \triangleright h_2)\end{aligned}$$

and $\bar{g} \sim (h_\ell \sqcup \cdots \sqcup h_1)$. Thus, $\bar{g}$ is completely reducible and, by the inductive assumption, completely transmutable. We have shown the leftmost $m-1$ factors of any complete decomposition of f are completely transmutable. Now we need only show that g_1 and g_2 are transmutable. We know $g_2 \oint \bar{g} = g_1 \triangleright (h_\ell \sqcup \cdots \sqcup h_2)$. By theorem 4.15, all complete decompositions of $g_1 \triangleright (h_\ell \sqcup \cdots \sqcup h_2)$ are simply decompositions of $h_\ell \sqcup \cdots \sqcup h_2$ transformed by g_1 (g_1 and $(h_\ell \sqcup \cdots \sqcup h_2)$ are composition-coprime). Therefore, $g_2 = g_1 \triangleright u$ for some $u \in \mathbb{A}_F$ similar to g_2, and g_1 and g_2 are transmutable. Thus, any completely reducible additive polynomial is completely transmutable.

We now show that if $f \in \mathbb{A}_F$ is completely transmutable then f is completely reducible. Once again we prove this by induction on the number of indecomposable factors in a complete decomposition of f. If $f = g_1$, where $g_1 \in \mathbb{A}_F$ is indecomposable, then f is obviously completely reducible. Assume the statement holds if f has fewer than m factors in a complete decomposition. Then assume $f = g_m \circ g_{m-1} \circ \cdots \circ g_1$ where $g_i \in \mathbb{A}_F$ for $1 \leq i \leq m$. Also, let $\bar{g} = g_m \circ g_{m-1} \circ \cdots \circ g_2$. Since $\bar{g}$ is completely transmutable, it is completely reducible by the inductive assumption, so $\bar{g} = h_\ell \sqcup \cdots \sqcup h_2$ where $\ell \in \mathbb{N}$ is greater than two and $h_2, \ldots, h_\ell \in \mathbb{A}_F$ are indecomposable. Each of the h_i are indecomposable right factors of $\bar{g}$ and because f is completely transmutable, each of the h_i's can be transmuted with g_1. Thus, $h_i = g_1 \triangleright \bar{h}_i$

for some $\bar{h}_i \in \mathbb{A}_F$, $\bar{h}_i \sim h_i$ for $1 \leq i \leq \ell$. Therefore

$$\begin{aligned} f = \bar{g} \circ g_1 &= (h_\ell \sqcup h_{\ell-1} \sqcup \cdots \sqcup h_2) \circ g_1 \\ &= ((g_1 \triangleright \bar{h}_\ell) \sqcup (g_1 \triangleright \bar{h}_{\ell-1}) \sqcup \cdots \sqcup (g_1 \triangleright \bar{h}_2)) \circ g_1 \\ &= \bar{h}_\ell \sqcup \bar{h}_{\ell-1} \sqcup \cdots \sqcup \bar{h}_2 \sqcup g_1, \end{aligned}$$

and since the $\bar{h}_i$ are indecomposable for $2 \leq i \leq \ell$ and g_1 is indecomposable, f is completely reducible. □

Note that since x^p does not transmute with itself, this theorem implies that any completely reducible polynomial can have at most one composition factor x^p in an arbitrary complete decomposition.
A strong relationship exists between the composition factors of an arbitrary complete decomposition and an arbitrary indecomposable basis.

Theorem 4.20. *Let $f \in \mathbb{A}_F$ be completely reducible, $(f, (f_m, f_{m-1}, \ldots, f_1)) \in cAPDEC_*^F$, and $h_1, \ldots, h_\ell$ be an indecomposable basis for f. Then $m = \ell$ and there exists a permutation σ of $\{1, \ldots, m\}$ such that $h_i \sim f_{\sigma_i}$ for $1 \leq i \leq m$.*

Proof. We proceed by induction on m. If $m = 1$, then f is indecomposable, and $\ell = 1$ and σ is the identity permutation. Now assume the hypothesis is true for all complete decompositions of length less than m. Let $f \in \mathbb{A}_F$ be completely reducible, $(f, (f_m, f_{m-1}, \ldots, f_1)) \in cAPDEC_*^F$, and $h_1, \ldots, h_\ell$ be an indecomposable basis for f. Since h_1 is an indecomposable right factor of f, there exists a decomposition $(f, (f'_m, f'_{m-1}, \ldots, f'_2, h_1)) \in cAPDEC_*^F$ and by corollary 4.17 a permutation τ of $\{1, \ldots, m\}$ such that $f'_i \sim f_{\tau_i}$ for $1 \leq i \leq m$. Now, $(f \not\phi h_1, (f'_m, f'_{m-1}, \ldots, f'_2)) \in cAPDEC_*^F$ and by the inductive assumption,

$$\begin{aligned} f \not\phi h_1 &= h_1 \sqcup (h_\ell \sqcup h_{\ell-1} \sqcup \cdots \sqcup h_2) \not\phi h_1 \\ &= h_1 \triangleright (h_\ell \sqcup h_{\ell-1} \sqcup \cdots \sqcup h_2) \\ &= (h_1 \triangleright h_\ell) \sqcup (h_1 \triangleright h_{\ell-1}) \sqcup \cdots \sqcup (h_1 \triangleright h_2), \end{aligned}$$

giving an indecomposable basis for $f \not\phi h_1$. By the inductive hypothesis $\ell - 1 = m - 1$ so $m = \ell$ and there exists a permutation μ of $\{2, \ldots, m\}$ such that $h_i \sim f'_{\mu_i}$ for $2 \leq i \leq m$. Extending this to a permutation $\bar{\mu}$ of $\{1, \ldots, m\}$ by letting $\bar{\mu}_1 = 1$ we find that $\sigma = \tau\bar{\mu}$ has the property that $h_i \sim f'_{\bar{\mu}_i} \sim f_{\sigma_i}$ for $1 \leq i \leq m$. □

4.5 The Uniqueness of Transmutation

A question which will concern us algorithmically is that of the uniqueness of transmutation. We can characterise how additive polynomials transmute in terms of the similar factors in an arbitrary complete decomposition. Let $g \in \mathbb{A}_F$ be monic of exponent ν with complete decomposition $(g, (g_m, g_{m-1}, \ldots, g_1)) \in cAPDEC_*^F$. Let $f \in \mathbb{A}_F$ be monic and indecomposable. Assume that f transmutes by g in two distinct ways, say $f = g \triangleright \bar{f}$ for $\bar{f} \in \mathbb{A}_F$, $\bar{f} \sim f$, and $f = g \triangleright \tilde{f}$ for $\tilde{f} \in \mathbb{A}_F$, $\tilde{f} \sim f$, and $\tilde{f} \neq \bar{f}$. Then $f \circ g$ has complete decompositions $(f \circ g, (\bar{g}_m, \ldots, \bar{g}_1, \bar{f}))$ where $\bar{g}_i \in \mathbb{A}_F$ and $\bar{g}_i \sim g_i$ for $1 \leq i \leq m$ and $(f \circ g, (\tilde{g}_m, \ldots, \tilde{g}_1, \tilde{f}))$ where $\tilde{g}_i \in \mathbb{A}_F$ and $\tilde{g}_i \sim g_i$ for $1 \leq i \leq m$. We know $\tilde{f} \nmid f \circ g$. Let $k \in \mathbb{N}$ be the smallest number such that $\tilde{f} \nmid \bar{g}_k \circ \bar{g}_{k-1} \circ \cdots \circ \bar{g}_1 \circ \bar{f}$ ($\tilde{f}$ does not divide $\bar{f}$). Then $\tilde{f}$ and $\bar{g}_{k-1} \circ \bar{g}_{k-2} \circ \cdots \circ \bar{g}_1 \circ \bar{f}$ are composition-coprime and by theorem 4.7, $\bar{g}_k = (\bar{g}_{k-1} \circ \cdots \circ \bar{g}_1) \triangleright \tilde{f}$ and $\bar{g}_k \sim \tilde{f}$. We have the following theorem:

Theorem 4.21. *Let $f, g \in \mathbb{A}_F$ be monic with $(g, (g_m, \ldots, g_1)) \in cAPDEC_*^F$ and f indecomposable. If f and g transmute in two or more distinct ways, then $f \sim g_i$ for some i such that $1 \leq i \leq m$.*

We can further characterise when non-unique transmutations occur by showing the following theorem about transmutations in general.

Theorem 4.22. *Let $f, g, h \in \mathbb{A}_F$ be monic. If f transmutes by $g \circ h$ with transmutation $\bar{f}$, then f and g transmute, and if a transmutation of f by g is $\tilde{f}$, then $\tilde{f}$ and h transmute as well.*

Proof. If $f = (g \circ h) \triangleright \bar{f}$, then $f = g \triangleright (h \triangleright \bar{f})$ by lemma 4.8. Since $\bar{f}$ and $g \circ h$ are composition-coprime, $\bar{f}$ and h are composition-coprime. Let $\tilde{f} = h \triangleright \bar{f}$. Then $\tilde{f}$ transmutes with g since $f = g \triangleright \tilde{f}$. Furthermore, because $\tilde{f} = h \triangleright \bar{f}$, $\tilde{f}$ and h transmute. $\square$

This theorem can be extended to the case when f transmutes by $h_m \circ h_{m-1} \circ \cdots \circ h_1$.

Theorem 4.23. *Let $f, h_i \in \mathbb{A}_F$ for $1 \leq i \leq m$. If f transmutes by $h = h_m \circ h_{m-1} \circ \cdots \circ h_1$, then*

(i) f transmutes by h_m, with transmutation $f^{(m)} \in \mathbb{A}_F$, for some $f^{(m)} \sim f$, and
(ii) for $m \geq i > 1$, $f^{(i)}$ transmutes by h_{i-1} with transmutation $f^{(i-1)} \in \mathbb{A}_F$ for some $f^{(i-1)} \sim f$.

Proof. We proceed by induction on m. The base case, where $m = 2$ follows directly from theorem 4.22. Assume the theorem holds if h is given as a composition of less than m factors. If h is given as a composition of m factors then by theorem 4.22 f transmutes by h_m . Let $f^{(m)} \in \mathbb{A}_F$ be the transmutation of f by h_m. Also by theorem 4.22, $f^{(m)}$ transmutes with $h_{m-1} \circ \cdots \circ h_1$. By the inductive hypothesis, $f^{(m)}$ transmutes by h_{m-1} with some transmutation $f^{(m-1)} \sim f$ and for $m - 1 \geq i > 1$, $f^{(i)}$ transmutes by h_{i-1} with some transmutation $f^{(i-1)} \sim f^{(m)} \sim f$. $\square$

If f transmutes by h in two distinct ways, then for an arbitrary decomposition $(h, (h_m, h_{m-1}, \ldots, h_1)) \in cAPDEC_*^F$, f transmutes by each h_i in turn for $m \geq i \geq 1$. Which transmutation of f by h is obtained is determined entirely by the transmutation of $f^{(i)}$ by h_i for $1 \leq i \leq m$. Since the transmutation of $f^{(i)}$ by h_i is unique if $f^{(i)} \nsim h_i$, the transmutation of f by h is determined completely by the transmutation of $f^{(i)}$ by h_i for $1 \leq i \leq m$ when $f^{(i)} \sim h_i$. With this in mind, we define an additive polynomial $f \in \mathbb{A}_F$ to be *similarity free* if in an arbitrary complete decomposition, no two of the composition factors are similar. In a similarity free additive polynomial, all transmutations of the factors are unique.

The previous theorem also allows us to strengthen theorem 4.16 of Ore's. We say two complete decompositions $(f, (f_m, f_{m-1}, \ldots, f_1))$ and $(f, (g_m, \ldots, g_1))$ in $cAPDEC_*^F$ are *single-indecomposable-transmutation equivalent* if $f_i = g_i$ for $1 \leq i \leq m$ or there exists an $\ell \in \mathbb{N}$ with $1 \leq \ell < m$ such that

$$(f, (g_m, \ldots, g_{\ell+1}, g_\ell, g_{\ell-1}, g_{\ell-2}, \ldots, g_1)) = (f, (f_m, \ldots, f_{\ell+1}, \bar{f}_{\ell-1}, \bar{f}_\ell, f_{\ell-2}, \ldots, f_1))$$

where $\bar{f}_\ell \sim f_\ell$ is the transmutation of f_ℓ by $f_{\ell-1}$ and $\bar{f}_{\ell-1} = \bar{f}_\ell \triangleright f_{\ell-1} \sim f_{\ell-1}$.

We define *indecomposable-transmutation equivalence* as the reflexive transitive closure of single-indecomposable-transmutation equivalence. Thus, two decompositions are indecomposable-transmutation equivalent if one can be obtained from the other by a sequence of transmutations of adjacent indecomposable factors.

Theorem 4.24. *Two complete decompositions are indecomposable- transmutation equivalent if and only if they are transmutation equivalent.*

Proof. If two complete decompositions are indecomposable-transmutation equivalent, then they are transmutation equivalent. By theorem 4.23, any

transmutation of an indecomposable additive polynomial with a composition of indecomposable polynomials is equivalent to a sequence of transmutations with each of the indecomposable factors in turn. Thus, single-transmutation equivalent decompositions are indecomposable-transmutation equivalent. Since transmutation equivalence is just the reflexive transitive closure of single-transmutation equivalence, transmutation equivalent decompositions must be indecomposable-transmutation equivalent. □

As an immediate corollary we get a stronger version of theorem 4.16.

Corollary 4.25. *All complete decompositions of an additive polynomial $f \in \mathbb{A}_F$ in $cAPDEC_*^F$ are indecomposable-transmutation equivalent.*

From now on we will simply say two complete decompositions are transmutation equivalent to mean indecomposable-transmutation equivalent.

4.6 The Number of Complete Decompositions

Using the methods from chapter 3 as well as the material from this chapter, we can now prove an upper bound on the number of complete decompositions of a (not necessarily simple) additive polynomial.

Let $f \in \mathbb{A}_F$ be monic of degree $n = p^\nu$. Then $f = g \circ x^{p^\ell}$ where $g \in \mathbb{A}_F$ is simple and $\ell \geq 0$. From theorem 3.10, we know that g has at most $n^{\mu \log n}$ complete decompositions in $cSAPDEC_*^F$ where $\mu = (2 \log p)^{-1}$. For each decomposition $(g, (g_m, g_{m-1}, \ldots, g_1)) \in cSAPDEC_*^F$, f has a decomposition

$$(f, (g_m, g_{m-1}, \ldots, g_1, \overbrace{x^p, x^p, \ldots, x^p}^{\ell \text{ times}})) \in cAPDEC_*^F.$$

Without changing the order of the g_i's for $m \geq i \geq 1$, and allowing for transformations into similar factors, we can distribute the indecomposable factors x^p throughout the decomposition of f. There are up to

$$\binom{m+\ell}{\ell} \leq \binom{\nu}{\ell} \leq 2^\nu \leq n$$

such distributions. We know these are all the decompositions because all decompositions of additive polynomials are transmutation equivalent. Because there are $n^{\mu \log n}$ complete decompositions of $g \in cSAPDEC_*^F$, there are at most $n^{1+\mu \log n}$ complete decompositions of $f \in cAPDEC_*^F$. We have shown the following generalisation of lemma 3.10.

Theorem 4.26. *If $f \in \mathbb{A}_F$ has degree n, then f has at most $n^{1+\mu \log n}$ decompositions in $cAPDEC_*^F$.*

Note that in the case of a perfect field F, for any $u \in \mathbb{A}_F$, we know $u \circ x^p = x^p \circ u^{\frac{1}{p}} = x^p \circ \bar{u}$ where $\bar{u} = u^{\frac{1}{p}} \circ x^p \in \mathbb{A}_F$. In this case there are, therefore, exactly $\binom{m+\ell}{\ell}$ times as many complete decomposition of f than of g in $cAPDEC_*^F$.

5 Decomposing Additive Polynomials

5.1 The Model of Computation

The model of computation used in this chapter is the "arithmetic Boolean circuit" as described in chapter 2, section A. Once again, let $\mathbf{S}_F(n)$ be the number of field operations required to factor an arbitrary univariate polynomial $f \in F[x]$ of degree n into irreducible factors (where F is a field of characteristic p). In this chapter, $\mathbf{S}_F(n)$ is assumed to be polynomially bounded. It is also assumed to satisfy the property that for $p, \nu \in \mathbb{N}$,

$$\sum_{0 \le i \le \nu} \mathbf{S}_F(p^i) = O(\mathbf{S}_F(p^\nu)).$$

The following theorem will also be useful in the analysis of some of our algorithms.

Lemma 5.1. *If $p, \nu, d \in \mathbb{N}$ with $p \ge 2$ and $\nu \ge 1$, then*

$$\sum_{1 \le i \le \nu} i^d p^i \le 3\nu^d p^\nu.$$

Proof. We proceed by induction on ν. If $\nu = 1$ then the theorem is trivially true. Assume it is true for $\nu < k$. Then

$$\begin{aligned}
\sum_{1 \le i \le k} i^d p^i &= \sum_{1 \le i \le k-1} i^d p^i + k^d p^k \\
&\le 3(k-1)^d p^{k-1} + k^d p^k \\
&\le (3/2) k^d p^k + k^d p^k \\
&\le 3k^d p^k,
\end{aligned}$$

and the theorem holds for all $\nu \ge 1$. □

5.2 The Cost of Basic Operations in $\mathbb{A}_F$.

Let $f, g \in \mathbb{A}_F$ be of exponents ν and ρ respectively, and $\max(\nu, \rho) \le \delta$. The following analyses of the basic operations in $\mathbb{A}_F$ are probably not optimal, but will be sufficient for our purposes.

Lemma 5.2. *(Composition) Computing $f \circ g$ requires at most $O(\delta^2 \log p)$ field operations.*

Proof. Each coefficient of g must be raised to the p^ith power for $0 \leq i \leq \nu \leq \delta$. This requires $O(\rho\delta \log p) = O(\delta^2 \log p)$ field operations. □

Lemma 5.3. *(Division with remainder) If $g \neq 0$, computing $Q, R \in \mathbb{A}_F$ such that $f = Q \circ g + R$ and $\operatorname{expn} R < \operatorname{expn} g$ requires $O(\delta^2 \log p)$ field operations.*

Proof. The cost of computing right division with remainder is dominated by the cost of raising g (and hence each coefficient of g) to the p^ith power for $0 \leq i \leq \nu - \rho$. This requires $O(\rho(\nu - \rho) \log p) = O(\delta^2 \log p)$ field operations. □

Lemma 5.4. *(Meet) Computing $f \sqcap g$ requires $O(\delta^3 \log p)$ field operations.*

Proof. In the Euclidean scheme described in the previous section, each step involves right division with remainder of additive polynomials with exponent at most δ. There are at most δ steps. Therefore we can compute the meet of f and g with $O(\delta^3 \log p)$ divisions. □

Lemma 5.5. *(Join) Computing $f \sqcup g$ requires $O(\delta^3 \log p)$ field operations.*

Proof. Using the formula of theorem 4.3, we must first compute the f_i's of the Euclidean scheme. This requires $O(\nu^3 \log p)$ field operations by the previous lemma. Computing the join then requires at most δ divisions and δ compositions of polynomials with exponents not exceeding 2δ. Thus, computing the join requires $O(\delta^3 \log p) + \delta O((2\delta)^2 \log p) = O(\delta^3 \log p)$ field operations. □

Lemma 5.6. *(Transformation) Computing $f \triangleright g$ requires $O(\delta^3 \log p)$ field operations.*

Proof. By definition $f \triangleright g = (f \sqcup g) \not\phi f$, and the number of field operations involved is dominated by the number of field operations required to compute the join, which is $O(\delta^3 \log p)$. □

5.3 The Minimal Additive Multiple

Let f be an arbitrary monic polynomial in $F[x]$. A concept which will prove extremely useful when dealing computationally with additive polynomials is that of the *minimal additive multiple* $\hat{f} \in \mathbb{A}_F$ of f. This is the monic additive polynomial of smallest exponent such that $\hat{f}$ is a multiple of f. The idea of a minimal additive multiple first appears in Ore[1933b].

If $f = 0$, then $\hat{f} = f = 0 \in \mathbb{A}_F$. If $f \in \mathbb{P}_F$ does not equal zero, the following algorithm computes the minimal additive multiple $\hat{f}$ of f.

```
MinAddMult :  P_F → A_F
    Input:  - f ∈ P_F of degree n ≥ 1.
    Output: - f̂ ∈ A_F, the minimal additive multiple of f.
    1) For i from 0 to n,
        1.1) compute h_i ≡ x^{p^i} mod f
             where h_i ∈ F[x] and deg h_i < deg f.
    2) Let k ∈ N be the smallest number with 0 ≤ k ≤ n
       such that there exists α_0, α_1, ..., α_{k-1} ∈ F
       such that h_k = Σ_{0≤j<k} α_j h_j.
    3) Return f̂ = x^{p^k} − Σ_{0≤j<k} α_j x^{p^j}.
```

We know $\hat{f}$ is a multiple of f because

$$\begin{aligned}\hat{f} &= x^{p^k} - \sum_{0\le j<k} \alpha_j x^{p^j} \\ &\equiv (h_k + \sum_{0\le j<k} \alpha_j h_j) \bmod f \\ &\equiv 0 \bmod f.\end{aligned}$$

The existence of any additive multiple of f with exponent $\ell < k$ would imply $h_0, \ldots, h_\ell$ are linearly dependent, which is false. Thus $\hat{f}$ is the minimal additive multiple of f. We know a solution always exists since $n+1$ vectors in F^n must be linearly dependent.

The number of field operations to compute h_j for $0 \le j \le n$ is $O(nM(n)\log p)$. The determination of k can be done by a modified Gaussian elimination on the $n \times n$ matrix H where H_{ij} is the coefficient of x^i in h_j for $0 \le i, j < n$. We proceed in stages from 0 to $n-1$. Let $H^{(0)} = H$. At stage ℓ (with $0 \le \ell < n$) we perform Guassian elimination on rows zero through ℓ of $H^{(k)}$ obtaining $H^{(k+1)}$ (leaving rows $\ell+1$ through $n-1$ unchanged). If, at the end of stage ℓ, row ℓ of $H^{(\ell+1)}$ has all entries zero, then rows zero through ℓ of H are linearly dependent and we can return $k = \ell$. At each stage of this elimination we only perform a row operation on row ℓ, so each stage requires $O(n^2)$ field operations over F. The complete procedure then requires $O(n^3)$ field operations. Given k, it is simple linear algebra to find $\alpha_0, \alpha_1, \ldots, \alpha_{k-1}$ such that $h_k = \sum_{0\le j<k} \alpha_j h_j$. This also require $O(n^3)$ field operations. We get the following theorem:

Theorem 5.7. *Let $f \in F[x]$ be monic of degree n. The minimal additive multiple $\hat{f} \in \mathbb{A}_F$ of f can be determined in $O(n^3)$ field operations.*

If $\tilde{f}$ is also an additive multiple of f, then by theorem 4.5, $h = \hat{f} \sqcap \tilde{f}$ is equal to the multiplicative greatest common divisor of $\hat{f}$ and $\tilde{f}$. Thus f divides $\hat{f} \sqcap \tilde{f}$ and this is an additive multiple of f. But $\hat{f}$ is the minimal additive multiple of f so $\hat{f} = \hat{f} \sqcap \tilde{f}$ and $\hat{f} \mathbin{\phi} \tilde{f}$. We have shown the following:

Theorem 5.8. *If $\hat{f} \in \mathbb{A}_F$ is the minimal additive multiple of $f \in F[x]$ and $\tilde{f}$ is a monic additive multiple of f, then $\hat{f} \mathbin{\phi} \tilde{f}$.*

Another characterisation of the minimal additive multiple of $f \in \mathbb{P}_F$ can be obtained by looking at the roots of f in its splitting field K. Assume f is squarefree and has roots $\{\theta_1, \ldots, \theta_n\}$ and minimal additive multiple h. Then f must have an additive multiple $g \in \mathbb{A}_K$ such that

$$g = ((x^p - \theta_1^{p-1}x) \sqcup (x^p - \theta_2^{p-1}x) \sqcup \cdots \sqcup (x^p - \theta_n^{p-1}x)) \in \mathbb{A}_K.$$

The polynomial g is an additive multiple of f because all roots of f are roots of g, and g is additive. Also, $g \mathbin{\phi} h$ because for each root θ_i of f, $k\theta_i$ must be a root of h for each $k \in \mathbb{Z}_p$ and $1 \leq i \leq n$. The one dimensional vector space $V_i = \{k\theta_i \mid k \in \mathbb{Z}_p\}$ is a subspace of the kernel of h, and the polynomial $g_i = x^p - \theta_i^{p-1}x$ has V_i as its kernel. So $g_i \mathbin{\phi} h$ for $1 \leq i \leq n$ and therefore $g = (g_1 \sqcup g_2 \sqcup \cdots \sqcup g_n) \mathbin{\phi} h$ as well (see lemma 4.1(v)). The coefficients of g are symmetric functions (over F) of the θ_i's for $1 \leq i \leq n$. Each automorphism of K relative to F carries the set of roots of f into itself. Thus, each automorphism leaves the coefficients of g fixed, and these coefficients must therefore be in F. It follows that $g \in F[x]$, and since g right divides h (the minimal additive multiple of f), g is equal to h. This also means that the exponent of the minimal additive multiple $\hat{f}$ is exactly the dimension of the linear span of the roots of f considered as a $\mathbb{Z}_p$ vector space in K.

An interesting case is when f is a normal polynomial in $\mathbb{Z}_p[x]$ (a normal polynomial is an irreducible polynomial such that its roots [in some fixed algebraic closure of $\mathbb{Z}_p$] form a basis over $\mathbb{Z}_p$ for its splitting field). The dimension of the $\mathbb{Z}_p$ vector space spanned by the roots of f is therefore the degree of f. It follows that the normal polynomials of degree n are exactly those irreducible polynomials whose minimal additive multiples have exponent n.

5.4 Complete Rational Decomposition of Additive Polynomials

Assume the field F supports a polynomial factorisation algorithm. The preceding method for finding minimal additive multiples can be used to build a polynomial time algorithm for finding rational complete normal decompositions of additive polynomials in a polynomial number of field operations.

First we present an algorithm for finding the set of indecomposable right composition factors of $f \in \mathbb{A}_F$.

```
FindIndecRightFactors:  A_F → P(A_F)
    Input:  - f ∈ A_F, a monic additive polynomial.
    Output: - H = {h_1, ..., h_ℓ}, the set of indecomposable
              right composition factors of f.
    1) Factor f such that f = x^{e_0} h_1^{e_1} h_2^{e_2} ··· h_m^{e_m}
       where h_i ∈ F[x] are distinct, monic and irreducible and
       e_i ∈ N \ {0} for 0 ≤ i ≤ m.
    2) Let J := {ĥ | ĥ is the minimal additive multiple of
                     h_i for some i such that 1 ≤ i ≤ ℓ}.
       Assume J = {g_1, ..., g_ℓ} for some ℓ ∈ N
       and is indexed such that if i < j then expn g_i ≤ expn g_j
       for 1 ≤ i ≤ ℓ.
    3) For 1 ≤ i < j ≤ ℓ, if g_i ϕ g_j, mark g_j.
    4) Let H = {g ∈ J | g not marked in step 3}.
    5) Return H.
```

To show correctness we must prove that $g \in H$ if and only if g is an indecomposable right composition factor of f. If $g \in \mathbb{A}_F$ is an indecomposable right factor of f, then, since g is also a multiplicative factor of f, each irreducible multiplicative factor $h \in F[x]$ of g is an irreducible multiplicative factor of f. We know that the minimal additive multiple $\hat{h} \in \mathbb{A}_F$ of any such h right divides g by theorem 5.8, and as g is indecomposable, $\hat{h} = g$. Therefore g will never be marked in step 3 and $g \in H$. Assume, on the other hand, that $g \in H$. Suppose that g is decomposable and h is an indecomposable right composition factor of g. Then h is an indecomposable right factor of f and $h \in H$ as shown above. In step 3, g would be marked as decomposable and would not be in H, a contradiction. Therefore, each $g \in H$ is indecomposable and the algorithm works correctly.

We now analyse the number of field operations required by the procedure `FindIndecRightFactors`. For $f \in \mathbb{A}_F$ of degree $n = p^\nu$ consider computing

`FindIndecRightFactors`(f). The factorisation in step 1 requires $O(\mathbf{S}_F(n))$ field operations. In step 2 we find additive multiples of each of the indecomposable right factors of f. The worst case occurs when there is one factor of degree $n-1$. Thus, step 2 requires $O(n^3)$ field operations. The number of operations required in the remaining steps is dominated by the requirements of steps 1 and 2, so we have the following:

Lemma 5.9. *Given $f \in F[x]$ of degree n we can compute all the indecomposable right factors of f in $O(\mathbf{S}_F(n) + n^3)$ field operations.*

Now consider the following algorithm for generating a complete decomposition of f in $cAPDEC_*^F$.

`CompleteDecomposition:` $\mathbb{A}_F \to cAPDEC_*^F$
`Input:` - $f \in \mathbb{A}_F$, `a monic additive polynomial.`
`Output:` - `a complete decomposition of` f `in` $cAPDEC_*^F$.
`1) Using FindRightIndecFactors, find the set` H `of indecomposable right factors of` f. `Assume` $H = \{h_1, \ldots, h_\ell\}$.
`2) If` $h_1 = f$
`then` f `is indecomposable, Return` $(f, (f))$.
`else`
`2.1) Let` $D :=$`CompleteDecomposition`$(f \not\phi h_1)$.
`We know` $D = (f \not\phi h_1, (u_t, \ldots, u_1)) \in cAPDEC_*^F$ `for some` $t \in \mathbb{N} \setminus \{0\}$.
`2.2) Return` $(f, (u_t, \ldots, u_1, h_1))$.

At each recursive stage of the algorithm we simply determine one indecomposable right factor h_1 of f. We then proceed recursively to find a complete decomposition of $f \not\phi h_1$. As f has exponent ν, and each indecomposable right factor has exponent at least one, there can be at most ν recursive stages. We now analyse the number of field operations required to decompose a polynomial $f \in \mathbb{A}_F$ of degree $n = p^\nu$. The worst case occurs when a $p - linear$ (exponent one) right composition factor occurs at each recursive stage i, for $1 \leq i \leq \nu$. In this case, at stage i we must call `FindRightIndecFactors` on a degree p^i polynomial, requiring $O(\mathbf{S}_F(p^i) + p^{3i})$ field operations. Thus, the total number of field operations required to find

one complete decomposition is

$$\sum_{0\le i\le \nu} (\mathbf{S}_F(p^i) + O(p^{3i})) = O(\mathbf{S}_F(p^\nu) + p^{3\nu}) \\ = O(\mathbf{S}_F(n) + n^3).$$

Theorem 5.10. *Given an additive polynomial $f \in \mathbb{A}_F$ of degree n we can determine a complete decomposition of f in $cAPDEC_*^F$ in $O(\mathbf{S}_F(n) + n^3)$ field operations.*

Corollary 5.11. *Rational indecomposability of an additive polynomial of degree n can be determined in $O(\mathbf{S}_F(n) + n^3)$ field operations.*

5.5 General Rational Decomposition of Additive Polynomials

Let $f \in \mathbb{A}_F$ be of degree n and let $\wp = (r_m, r_{m-1}, \ldots, r_1)$ be an ordered factorisation of n. The fact that we can obtain a complete decomposition of an $f \in cAPDEC_*^F$ in a polynomial number of field operations in n does not mean that we can determine the existence of a decomposition of f in $APDEC_\wp^F$, and find one if it exists, in polynomial time. We can look at the set of all complete decompositions and check if the composition factors of any of them can be "grouped" according to the desired ordered factorisation $\wp$. More generally, a length d ordered factorisation $\kappa = (s_d, s_{d-1}, \ldots, s_1)$ of $n \in \mathbb{N}$ is said to be a *refinement* of a length $m \le d$ ordered factorisation $\wp = (r_m, r_{m-1}, \ldots, r_1)$ if there exists a non-decreasing, onto map $\varphi : \{1, \ldots, d\} \to \{1, \ldots, m\}$ such that for $1 \le j \le m$,

$$\prod_{\substack{1\le i\le d \\ \varphi(i)=j}} s_i = r_j.$$

This is simply saying that the d-tuple κ can be divided into m contiguous pieces, with the elements of piece j having product r_j, for $1 \le j \le m$. One approach to finding decompositions of f with a given ordered factorisation is to generate the set of all complete decompositions of f and check if any of the ordered factorisations associated with these decompositions are a refinement of $\wp$.

We now present an algorithm for generating all the complete decompositions of an additive polynomial.

```
AllCompleteDecomposition: 𝔸_F → P(cAPDEC*^F)
    Input:  - f ∈ 𝔸_F, a monic additive polynomial.
    Output: - the set of all complete decompositions of f
              in cAPDEC*^F.
    1) Using FindRightIndecFactors, find the set H of
       indecomposable right factors of f.  Assume
       H = {h_1, ..., h_ℓ}.
    2) If f = h_1
          Then f is indecomposable, Return (f, (f)).
          Else
             2.1) Let T := ∅.
             2.2) For i from 1 to ℓ
                  2.2.1) Let D^(i) :=CompleteDecomposition(f ∮ h_i),
                         the set of all complete decompositions
                         of (f ∮ h_i) in cAPDEC*^F.
                  2.2.2) For each decomposition
                         (f ∮ h_i, (u_ℓ, ..., u_1)) ∈ D^(i),
                         add (f, (u_ℓ, ..., u_1, h_i)) ∈ cAPDEC*^F
                         to T.
             2.3) Return T.
```

Correctness is easy to verify. At each recursive stage we simply find the set of all indecomposable right factors H of f and for each $h \in H$ we recursively find the complete decompositions of $f \not\circ h$. All complete decompositions are found and, since we choose a different member of H in each step 2.2.1, each decomposition added to T is distinct.

We analyse the cost of the algorithm by first finding the cost of computing one complete decomposition. We then use the bounds developed in chapter 3 and 4 on the number of complete decompositions to get bounds on the cost of computing all complete decompositions. As with `CompleteDecomposition`, the worst case occurs when a $p - linear$ right composition factor occurs at each recursive stage i, for $1 \leq i \leq \nu$. In this case, at stage i, we must call `FindRightIndecFactors` on a degree p^i polynomial, requiring $O(\mathbf{S}_F(p^i)+p^{3i})$ field operations. Thus the total number of field operations required to find

one complete decomposition is

$$\sum_{0\le i\le \nu} \mathbf{S}_F(p^i) + O(p^{3i}) = O(\mathbf{S}_F(p^\nu) + p^{3\nu}) \\ = O(\mathbf{S}_F(n) + n^3).$$

Theorem 5.12. *If $f \in \mathbb{A}_F$ is monic of degree n and $t \in \mathbb{N}$, then we can determine if there exist t decompositions of f in $cAPDEC_*^F$, and if so find them, with $O(t(\mathbf{S}_F(n) + n^3))$ field operations.*

By theorem 4.26, the total number of complete normal decompositions of f in $cAPDEC_*^F$ is $n^{O(\log n)}$, so we can compute all complete rational decompositions of an arbitrary additive polynomial in a quasi-polynomial number of field operations.

Let $\wp$ be a given ordered factorisation of n. As we generate each complete decomposition of f, we can check if the ordered factorisation associated with it is a refinement of $\wp$. The number of operations required to do this is dominated by the other steps in the algorithm. Thus, the number of operations required to find all decompositions of f in $DEC_\wp^F$ is of the same order as the number required to generate all complete decompositions.

Corollary 5.13. *If $f \in \mathbb{A}_F$ is monic of degree n, and $\wp$ is an ordered factorisation of n, then all decompositions of f in $APDEC_\wp^F$ can be found in $n^{O(\log n)}$ field operations.*

Note that this algorithm requires a comparable number of operations to those of Kozen and Landau[1986] for separable irreducible polynomials.

5.6 General Decomposition of Completely Reducible Additive Polynomials

We now consider computing decompositions of a completely reducible additive polynomial $f \in \mathbb{A}_F$ of degree n corresponding to a given ordered factorisation $\wp$ of n. We will see that the decomposition problem for completely reducible additive polynomials can be computed in a polynomial number of field operations in the input degree. We proceed by constructing an indecomposable basis for f (see chapter 4, section D) and combine the basis components appropriately to determine if an appropriate decomposition exists, and if so, find it.

We now describe an efficient way of computing an indecomposable basis for a given completely reducible additive polynomial. The procedure strongly resembles the one described in the proof of lemma 4.18.

```
IndecBasis:  𝔸_F → 𝔸_F*
    Input:    f ∈ 𝔸_F, completely reducible of degree n = p^ν.
    Output:   u_1, u_2, ..., u_d ∈ 𝔸_F, an indecomposable basis for f.
    1) Using FindIndecRightFactors, find the set
       R = {v_1, v_2, ..., v_ℓ} of indecomposable right factors of f.
    2) Let j := 0.
    3) Let g^(0) := x.
    4) For i from 1 to ℓ do
        4.1) If v_i ⊓ g^(i-1) = x then
                4.1.1) Let g^(i) := g^(i-1) ⊔ v_i.
                4.1.2) Let j := j + 1.
                4.1.3) Let u_j := v_i.
               Else
                4.1.4) Let g^(i) := g^(i-1).
        4.2) If g^(i) = f then quit,
                  returning u_1, ..., u_j as an indecomposable basis.
```

Since we know f is completely reducible, f is, by definition, the join of its indecomposable right factors $v_1, \ldots, v_\ell$. The algorithm simply looks at each indecomposable right factor in turn. At step 4.1, either $v_i \sqcap g^{(i-1)} = x$ or $v_i \sqcup g^{(i-1)} = g^{(i-1)}$. Only in the first case does v_i contribute anything to the join of all the right factors, and, in this case, $\mathrm{expn}(g^{(i)}) = \mathrm{expn}(g^{(i-1)}) + \mathrm{expn}(v_i)$. The set of all such contributing right factors clearly forms an indecomposable basis for f. The cost of this algorithm is dominated by the cost of finding the set of indecomposable right factors of f. We have shown the following:

Lemma 5.14. *Let $f \in \mathbb{A}_F$ be completely reducible of degree n. We can find an indecomposable basis for f with $O(\mathbf{S}_F(n) + n^3)$ field operations.*

Let $f \in \mathbb{A}_F$ be completely reducible of degree $n = p^\nu$ and let $\wp = (p^{\rho_m}, \ldots, p^{\rho_1})$ be an ordered factorisation of n. We now address the problem of finding a decomposition of f in $APDEC^F_\wp$. It is true in general that there exists a decomposition of f in $APDEC^F_\wp$ if and only if there exists an ordered factorisation $\kappa = (p^{\sigma_d}, p^{\sigma_{d-1}}, \ldots, p^{\sigma_1})$ of n which is a refinement of

$\wp$ such that f has a complete decomposition in $cAPDEC^F_\kappa$. Since all completely reducible additive polynomials are completely transmutable, we need only determine if some permutation of the ordered factorisation κ is a refinement of $\wp$. By theorem 4.20, the composition factors of an arbitrary complete decomposition and the members of an arbitrary indecomposable basis of f are similar in pairs. Assume $u_1, \ldots, u_d$ forms an indecomposable basis for f, where $\deg u_i = p^{e_i}$ for $1 \leq i \leq d$. Then f has a decomposition in $APDEC^F_\wp$ if an only if some permutation of $\mu = (p^{e_d}, p^{e_{d-1}}, \ldots, p^{e_1})$ is a refinement of $\wp$. This is equivalent to saying that some permutation of μ is a refinement of some permutation of $\wp$ – we do not need to consider the order of $\wp$ either. In light of this, we denote an *unordered factorisation* of n of length m as $[a_m, a_{m-1}, \ldots, a_1]$ where $a_i \in \mathbb{N}$ for $1 \leq i \leq m$, $\prod_{1 \leq i \leq m} a_i = n$ and for any permutation τ of $\{1 \ldots m\}$, $[a_{\tau_m}, a_{\tau_{m-1}}, \ldots, a_{\tau_1}] = [a_m, a_{m-1}, \ldots, a_1]$. Such a data structure can be easily managed computationally and the details will be left to the reader (for instance, one could manage them as sorted m tuples). Basic operations on an unordered factorisation of length ℓ, such as assignment and equality test, will be assumed to require $\ell^{O(1)}$ field operations. Let $\bar{\wp} = [p^{\rho_m}, p^{\rho_{m-1}}, \ldots, p^{\rho_1}]$ and $\bar{\mu} = [p^{e_d}, p^{e_{d-1}}, \ldots, p^{e_1}]$ be the unordered factorisations corresponding with $\wp$ and μ respectively. A length d unordered factorisation $\gamma = [p^{\sigma_d}, p^{\sigma_{d-1}}, \ldots, p^{\sigma_1}]$ is an *unordered refinement* of $\bar{\wp}$ if there is an onto map $\psi : \{1, \ldots, d\} \to \{1, \ldots m\}$ such that for $1 \leq j \leq m$,

$$\prod_{\substack{1 \leq i \leq d \\ \psi(i) = j}} \sigma_i = r_j.$$

We proceed by generating the set L of all length m unordered factorisations λ of n which are unordered refinements of $\bar{\mu}$. For each $\lambda \in L$ we keep exactly one refinement ψ_λ from $\bar{\mu}$ to λ, ignoring other such refinements. We show that L is in fact small and can be computed in time polynomial in n. Once L is computed, it is easy to check if $\bar{\wp}$ is in L. If it is, then f has a decomposition in $APDEC^F_\wp$ and it is a simple matter to recover this decomposition from the refinement.

We proceed by dynamic programming. We define the $d \times m$ array S of sets of unordered factorisations as follows. For $1 \leq i \leq d$ and $1 \leq j \leq m$, let S_{ij} be the set of unordered factorisations of length j of p^{d_i} (where $d_i = \sum_{1 \leq k \leq i} e_i$) which are unordered refinements of $[p^{e_i}, p^{e_i - 1}, \ldots, p^{e_1}]$. The following algorithm exploits an easy recurrence to generate all of S.

```
FindUnorderedFacts:  ℕ* × ℕ → (P(ℕ*))*
    Input:  - μ = (p^{e_d}, p^{e_{d-1}}, ..., p^{e_1}), an ordered
              factorisation of n,
            - m ∈ ℕ, an integer at most d.
    Output: - S, a d × m array of sets of unordered
              factorisations of n as described above.
    1) S_11 := (p^{e_1}).
       For i from 2 to d
           For j from 1 to m
               2) S_ij := ∅.
               3) For each unordered factorisation
                  [p^{a_{j-1}}, ..., p^{a_1}] ∈ S_{i-1,j-1}
                  add [p^{a_{j-1}}, ..., p^{a_1}, p^{e_i}] to S_ij.
               4) For each unordered factorisation
                  [p^{a_j}, ..., p^{a_1}] ∈ S_{i-1,j} and for 1 ≤ k ≤ j
                  add [p^{a_j}, ..., p^{a_{k+1}}, p^{a_k}p^{e_i}, p^{a_{k-1}}, ..., p^{a_1}] to S_ij.
```

Certainly, at the conclusion S_{dm} contains the desired set of unordered factorisations. The number of unordered factorisations which are unordered refinements of $\bar{\mu}$ is at most the number of additive partitions $p(\nu)$ of ν (the exponents of p in the unordered factorisation give a partition of ν). Hua[1982] (theorem 6.1) shows that

$$\begin{aligned} p(\nu) &\leq \nu^{3\lfloor\sqrt{\nu}\rfloor} \\ &\leq \nu^{3\sqrt{\nu}+3} \\ &\leq (2^{\log\nu})^{3\sqrt{\nu}+3} \\ &\leq 2^{6\sqrt{\nu}\log\nu}. \end{aligned}$$

Thus the total algorithm can be completed in

$$\begin{aligned} dm\nu^{O(1)}2^{6\sqrt{\nu}\log\nu} &= \nu^{O(1)}2^{6\sqrt{\nu}\log\nu} \\ &= O(n) \end{aligned}$$

field operations. By keeping the products $p^{a_k}p^{e_i}$ in step 4 in an "unevaluated" form (or, alternatively, keeping some record of the multiplicands) for each $\lambda \in L$, we can easily recover an explicit unordered refinement ψ_λ from $\bar{\mu}$ to λ. By checking if $\bar{\varphi}$ is in S_{dm}, we can determine if $\bar{\mu}$ is an unordered refinement of $\bar{\varphi}$, and, if it is, actually determine the refinement ψ.

Assume $\bar{\wp} \in S_{dm}$ and ψ is an unordered refinement from $\bar{\mu}$ to $\bar{\wp}$. For $1 \leq j \leq m$, let

$$h_j = \bigsqcup_{\substack{1 \leq i \leq d \\ \varphi(i)=j}} u_i.$$

Then for $1 \leq i \leq m$, $\deg h_i = r_i$, $h_1, h_2, \ldots, h_m$ are pairwise composition coprime, and $h_1 \sqcup \cdots \sqcup h_m = f$. The following simple procedure can be used to recover a decomposition of f in $APDEC^F_{\wp}$.

```
BasisToDec:  A_F* → APDEC*_F
    Input:  - h_1, ..., h_m ∈ A_F such that f = h_1 ⊔ h_2 ⊔ ··· ⊔ h_m,
              h_i ⊓ h_j = x for 1 ≤ i < j ≤ m
              and deg h_i = r_i for 1 ≤ i ≤ m.
    Output: - (f, (f_m, f_{m-1}, ..., f_1)) ∈ APDEC^F_℘
              where ℘ = (r_m, r_{m-1}, ..., r_1).
    Let g^(0) := x.
    For 1 ≤ i ≤ m
        Let g^(i) := g^(i-1) ⊔ h_i.
        Let f_i := g^(i) ∮ g^(i-1).
    Return (f, (f_m, f_{m-1}, ..., f_1)) ∈ APDEC^F_℘.
```

This procedure can certainly be completed in $O(n^3)$ field operations. We have now completed the description of a general decomposition algorithm for completely reducible additive polynomials and have shown the following theorem:

Theorem 5.15. *Given $f \in \mathbb{A}_F$ completely reducible of degree n and $\wp$ an ordered factorisation of n, we can determine if f has a decomposition in $APDEC^F_{\wp}$, and if so find one, in $O(\mathbf{S}_F(n) + n^3)$ field operations.*

5.7 Determining Transmutations of Additive Polynomials

Another approach to finding decompositions of additive polynomials is to find one complete decomposition and then, using the relationship between decompositions (developed in chapter 4), produce a decomposition into factors of the desired degrees.

To do this we must be able to determine if two polynomials $f, g \in \mathbb{A}_F$ are transmutable, and find the set

$$\{(\bar{g}, \bar{f}) \in \mathbb{A}_F \times \mathbb{A}_F \mid \bar{f} \sim f,\ f = g \triangleright \bar{f}, \bar{g} = \bar{f} \triangleright g\},$$

of possible transmutations of f by g. The following algorithm performs this task if f is indecomposable in a polynomial number of operations in the sum of the degrees of f and g.

```
Transmutable:  𝔸_F × 𝔸_F → P(𝔸_F × 𝔸_F)
    Input:  - f ∈ 𝔸_F, monic and indecomposable, g ∈ 𝔸_F, monic.
    Output: - T = {(ḡ, f̄) ∈ 𝔸_F × 𝔸_F | f̄ ~ f, f = g ▷ f̄, ḡ = f̄ ▷ g}.
    1) Using FindIndecRightFactors, find the set H ⊆ 𝔸_F of
       indecomposable right factors of f ∘ g.
    2) Let J := {f̂ ∈ H | expn f̂ = expn f} ⊆ H.
    3) Let T := ∅.
    4) For each f̂ ∈ J
        4.1) Let ĝ := (f ∘ g) ∅ f̂.
        4.2) If ĝ = f̂ ▷ g then let T := T ∪ (ĝ, ĥ).
    5) Return T.
```

A transmutation of f by g will transform f into a similar polynomial $\hat{f} \in \mathbb{A}_F$ which is a right factor of $f \circ g$. Therefore, we eliminate all the $\hat{f} \in H$ with exponents unequal to that of f in step 2. Now, for any $\hat{g}, \hat{f} \in \mathbb{A}_F$ such that $f \circ g = \hat{g} \circ \hat{f}$ and $\hat{g} = \hat{f} \triangleright g$, we know

$$\begin{aligned} f \circ g &= (\hat{f} \triangleright g) \circ \hat{f} \\ &= \hat{f} \sqcup g \\ &= ((g \sqcup \hat{f}) \not\triangleright g) \circ g \\ &= (g \triangleright \hat{f}) \circ g. \end{aligned}$$

It follows that $f = g \triangleright \hat{f}$, and since f and $\hat{f}$ have the same exponent, g and $\hat{f}$ are composition coprime and f transmutes by g.

Theorem 5.16. *The set of all transmutations of an indecomposable additive polynomial $f \in \mathbb{A}_F$ by an arbitrary additive polynomial $g \in \mathbb{A}_F$, where the degree of $f \circ g$ is $n = p^\nu$, can be computed in $O(\mathbf{S}_F(n) + n^3)$ field operations.*

Proof. Determining the set of indecomposable right factors in step 1 requires $O(\mathbf{S}_F(p^\nu) + p^{3\nu}) = O(\mathbf{S}_F(n) + n^3)$. Step 4.1 require $O(n)$ exponent ν divisions, and $O(n\nu^2 \log p)$ field operations. Finally, step 4.2 requires $O(n\nu^3 \log p)$ field operations. Thus the total number of field operations required is dominated by the number required for step 1 and is $O(\mathbf{S}_F(n) + n^3)$. □

Suppose $g \in \mathbb{A}_F$ in the above algorithm is given as a complete decomposition. Then, if f transmute by g, $f = g \triangleright \bar{f}$ where $\bar{f} \in \mathbb{A}_F$ and $\bar{f} \sim f$. It follows that $f \circ g = \bar{g} \circ \bar{f}$ where $\bar{g} = \bar{f} \triangleright g$. We would like to give the corresponding decomposition of $\bar{g}$. By theorem 4.13 we can compute the effect of transformation of a composition. The following algorithm performs this task efficiently.

`TransformComposition:` $\mathbb{A}_F \times cAPDEC_*^F \to cAPDEC_*^F$
`Input:` - $h \in \mathbb{A}_F$, `monic and indecomposable,`
- $(g, (g_m, g_{m-1}, \ldots, g_1)) \in cAPDEC_*^F$.
`Output:` - $(\bar{g}, (\bar{g}_m, \bar{g}_{m-1}, \ldots, \bar{g}_1)) \in cAPDEC_*^F$ `where`
$\bar{g} = h \triangleright g$ `and` $\bar{g}_i \in \mathbb{A}_F$, $\bar{g}_i \sim g_i$ `for` $1 \le i \le m$.
$h_1 := h$.
$\bar{g}_1 := h_1 \triangleright g_1$.
`For` $2 \le i \le m$
$h_i := (g_{i-1} \circ g_{i-2} \circ \cdots \circ g_1) \triangleright h$.
$\bar{g}_i := h_i \triangleright g_i$.
`Return` $(h \triangleright g, (\bar{g}_m, \bar{g}_{m-1}, \ldots, \bar{g}_1))$.

Correctness follows immediately as the algorithm is simply a direct application of theorem 4.13. If $g \in \mathbb{A}_F$ and $h \in \mathbb{A}_F$ are of exponents ρ and σ respectively and $\delta = \max(\rho, \sigma)$, then computing $h_i \in \mathbb{A}_F$ in the algorithm requires $O(\delta^3 \log p)$ field operations for each i with $1 \le i \le m$. Computing $\bar{g}_i$ also requires $O(\delta^3 \log p)$ field operations for each i with $1 \le i \le m$. We know that $m \le \delta$, so we get the following theorem:

Theorem 5.17. *If $(g, (g_m, g_{m-1}, \ldots, g_1)) \in cAPDEC_*^F$ where $g \in \mathbb{A}_F$ has exponent ρ, and $h \in \mathbb{A}_F$ has exponent σ, then we can transform the decomposition of g into a corresponding decomposition of $h \triangleright g$ in $O(\delta^4 \log p)$ field operations, where $\delta = \rho + \sigma$.*

5.8 Bidecomposition of Similarity Free Additive Polynomials

We now describe an algorithm for finding a bidecomposition of a similarity free additive polynomial $f \in \mathbb{A}_F$ of degree $n = p^\nu$ corresponding to an ordered factorisation $\wp = (p^\rho, p^\sigma)$. We will see this can be done in a polynomial number of field operations in the degree of the input polynomial. Using the algorithm `CompleteDecomposition`, we can find a complete decomposition $(f, (f_m, f_{m-1}, \ldots, f_1)) \in cAPDEC_*^F$ with $O(\mathbf{S}_F(n) + n^3)$ field operations. We

proceed by looking at each subset $S \subseteq \{1, \ldots, m\}$ such that $\sum_{i \in S} \text{expn } f_i = \sigma$. Assume S has cardinality $t \in \mathbb{N}$ where $t \geq 1$. For each S we determine if there exists a decomposition $(f, (g_m, \ldots, g_1)) \in cAPDEC_*^F$ and a bijection φ between $\{1, \ldots, t\}$ and S with $g_i \sim f_{\varphi(i)}$ for $1 \leq i \leq t$. Say a decomposition with this property is *consistent* with S and $(f, (f_m, f_{m-1}, \ldots, f_1))$. In other words, there is a decomposition such that the rightmost t composition factors are similar in pairs to the composition factors indexed by S. Because we are assuming f is similarity free, all transmutations are unique (see chapter 4, section E).

In the following algorithm we determine if a decomposition consistent with a given S of size t and $(f, (f_m, f_{m-1}, \ldots, f_1)) \in cAPDEC_*^F$ exists. The algorithm proceeds in stages ℓ, for $1 \leq \ell \leq t$. Assume $(f_m^{(0)}, f_{m-1}^{(0)}, \ldots, f_1^{(0)}) = (f_m, f_{m-1}, \ldots, f_1)$. At each stage ℓ we transmute one of the factors of $(f, (f_m^{(\ell-1)}, f_{m-1}^{(\ell-1)}, \ldots, f_1^{(\ell-1)}))$ which is similar to a factor indexed in S into the the ℓ^{th} composition factor position from the right, obtaining a new decomposition $(f, (f_m^{(\ell)}, f_{m-1}^{(\ell)}, \ldots, f_1^{(\ell)}))$. We keep track of where the factors of the original decomposition have been transmuted to at the end of stage ℓ by means of an index vector $c^{(\ell)} = (c_m^{(\ell)}, \ldots, c_1^{(\ell)})$. At this point, $f_j^{(\ell)} \sim f_{c_j^{(\ell)}}$ for each j such that $1 \leq j \leq m$. The decomposition produced at the end of stage ℓ will have the property that for each $j \in \mathbb{N}$ such that $1 \leq j \leq \ell$, $c_j^{(\ell)} \in S$. If at each stage such a decomposition can be found, at stage t we will have a decomposition of f consistent with S and $(f, (f_m, f_{m-1}, \ldots, f_1))$.

`FactorsToRight:` $cAPDEC_*^F \times \mathbf{P}(\mathbb{N}) \to cAPDEC_*^F$

`Input:` - $(f, (f_m, f_{m-1}, \ldots, f_1)) \in cAPDEC_*^F$,
- $S \subseteq \mathbb{N}$ `of cardinality` $t \in \mathbb{N}$.

`Output:` - $(f, (g_m, g_{m-1}, \ldots, g_1)) \in cAPDEC_*^F$ `consistent with` $(f, (f_m, f_{m-1}, \ldots, f_1))$ `and` S `(if such a decomposition exists).`

`1) Let` $c^{(0)} := (c_m^{(0)}, c_{m-1}^{(0)}, \ldots, c_1^{(0)}) := (m, m-1, \ldots, 1)$.

`2) Let` $S^{(0)} := S$.

`3) For` ℓ `from 1 to` t

`3.1) For each` $i \in S^{(\ell-1)}$

`3.1.1) Let` $k \in \mathbb{N}$ `be such that` $c_k^{(\ell-1)} = i$.

`3.1.2) Using Transmutable, determine if` $f_k^{(\ell-1)}$ `transmutes by` $f_{k-1}^{(\ell-1)} \circ \cdots \circ f_\ell^{(\ell-1)}$.

If so, goto step 3.3.

3.2) No transmutation found, quit.

3.3) Using TransformComposition, for $\ell \leq j \leq k$ find $\bar{f}_j^{(\ell-1)} \sim f_j^{(\ell-1)}$ such that $f_k^{(\ell-1)} \circ f_{k-1}^{(\ell-1)} \circ \cdots \circ f_\ell^{(\ell-1)} = \bar{f}_{k-1}^{(\ell-1)} \circ \bar{f}_{k-2}^{(\ell-1)} \circ \cdots \circ \bar{f}_\ell^{(\ell-1)} \circ \bar{f}_k^{(\ell-1)}$ (ie. compute the transmutation of $f_k^{(\ell-1)}$ by $\bar{f}_{k-1}^{(\ell-1)} \circ \bar{f}_{k-2}^{(\ell-1)} \circ \cdots \circ \bar{f}_\ell^{(\ell-1)}$).

3.4) Let $(f_m^{(\ell)}, \ldots, f_1^{(\ell)}) := (f_m^{(\ell-1)}, \ldots, f_{k+1}^{(\ell-1)}, \bar{f}_{k-1}^{(\ell-1)}, \ldots, \bar{f}_\ell^{(\ell-1)}, \bar{f}_k^{(\ell-1)}, f_{\ell-1}^{(\ell-1)}, \ldots, f_1^{(\ell-1)})$.

3.5) Let $c^{(\ell)} := (c_m^{(\ell-1)}, \ldots, c_{k+1}^{(\ell-1)}, c_{k-1}^{(\ell-1)}, \ldots, c_\ell^{(\ell-1)}, c_k^{(\ell-1)}, c_{\ell-1}^{(\ell-1)}, \ldots, c_1^{(\ell-1)})$.

3.6) Let $S^{(\ell)} := S^{(\ell-1)} - \{i\}$.

4) Return $(f, (f_m^{(t)}, f_{m-1}^{(t)}, \ldots, f_1^{(t)}))$.

We now show the correctness of the above algorithm. If there exists no decomposition of f consistent with $(f, (f_m, f_{m-1}, \ldots, f_1))$ and S, then FactorsToRight will obviously not find it.

Lemma 5.18. *Let S be a subset of $\{1, \ldots m\}$. If there exists a decomposition of f consistent with $(f, (f_m, f_{m-1}, \ldots, f_1))$ and S,* FactorsToRight *will find one.*

Proof. We prove this lemma by induction on t, the cardinality of S. For the basis step, $t = 1$ and $S = \{i\}$ for some i such that $1 \leq i \leq m$. Assume that $(f, (g_m, g_{m-1}, \ldots, g_1)) \in cAPDEC_*^F$ is a decomposition of f consistent with $(f, (f_m, f_{m-1}, \ldots, f_1))$ and S. In step 3.1.1, $k = i$. We know that $g_1 \nmid f$. Let $j \in \mathbb{N}$ be the smallest number such that $g_1 \nmid f_j^{(0)} \circ \cdots \circ f_1^{(0)}$. The polynomials g_1 and $f_{j-1}^{(0)} \circ \cdots \circ f_1^{(0)}$ are composition-coprime, so by theorem 4.7, $f_j^{(0)} = (f_{j-1}^{(0)} \circ \cdots \circ f_1^{(0)}) \triangleright g_1$, $f_j^{(0)} \sim g_1$, and $f_j^{(0)}$ transmutes by $f_{j-1}^{(0)} \circ \cdots \circ f_1^{(0)}$. Since f is assumed to be similarity free, $j = k$ and the transmutation of step 3.1 gives a decomposition consistent with $(f, (f_m, f_{m-1}, \ldots, f_1))$ and S.

Now assume that FactorsToRight finds a decomposition of f consistent with $(f, (f_m, f_{m-1}, \ldots, f_1))$ and S if the cardinality of S is less than t. We must show it does so for S of cardinality t as well.

Assume S has cardinality t and that $(f, (g_m, g_{m-1}, \ldots, g_1)) \in cAPDEC_*^F$ is a decomposition of f consistent with $(f, (f_m, f_{m-1}, \ldots, f_1))$ and S. With

$\ell = 1$ we know there exists a $k \in S$ such that $f_k^{(0)} \sim g_1$ and by the argument for the basis case, $f_k^{(0)} = (f_{k-1}^{(0)} \circ \cdots \circ f_1^{(0)}) \triangleright g_1$ and $f_k^{(0)}$ transmutes by $f_{k-1}^{(0)} \circ \cdots \circ f_1^{(0)}$. The algorithm may or may not transmute $f_k^{(0)}$ to the right of the decomposition, depending on the choice in step 3.1. Assuming we do choose this $f_k^{(0)}$ to transmute in step 3.1, we get

$$\begin{aligned}(f_m^{(1)}, \ldots, f_1^{(1)}) &= (f_m^{(0)}, \ldots, f_{k+1}^{(0)}, \bar{f}_{k-1}^{(0)}, \ldots, \bar{f}_1^{(0)}, \bar{f}_k^{(0)}) \\ &= (f_m^{(0)}, \ldots, f_{k+1}^{(0)}, \bar{f}_{k-1}^{(0)}, \ldots, \bar{f}_1^{(0)}, g_1)\end{aligned}$$

where $\bar{f}_i^{(0)} \sim f_i$ for $1 \leq i \leq k$ (we know $f_k^{(0)} = g_1$ because f is similarity free). As g_1 is never referenced in the computation again, the remainder of the algorithm is essentially finding a decomposition of $f \not\phi g_1$ (which has decomposition $(f \not\phi g_1, (f_m^{(1)}, \ldots, f_2^{(1)})) \in cAPDEC_*^F$) that is consistent with $(f_m^{(1)}, f_{m-1}^{(1)}, \ldots, f_2^{(1)})$ and $S - \{i\}$. Since $S - \{i\}$ has cardinality less than t, `FactorsToRight` finds such a decomposition by the inductive hypothesis.

Suppose, however, that in step 3.1, with $\ell = 1$, we transmute $f_w^{(0)} \nsim g_1$, for some w such that $1 \leq w \leq m$, $w \in S$ and $w \neq k$, to the right. Then $f_w \sim g_j$ for some $j \leq t$. Since we know $\bar{f}_w^{(0)} \not\phi f$, g_j transmutes by $g_{j-1} \circ \cdots \circ g_1$. Assume

$$g_j \circ (g_{j-1} \circ \cdots \circ g_1) = \bar{g}_{j-1} \circ \cdots \circ \bar{g}_1 \circ \bar{g}_j$$

where $g_v \sim \bar{g}_v$ for $1 \leq v \leq j$. Then

$$(f, (g_m, g_{m-1}, \ldots, g_{j+1}, \bar{g}_{j-1}, \ldots, \bar{g}_1, \bar{g}_j)) \in cAPDEC_*^F$$

must be another decomposition of f consistent with $(f, (f_m, f_{m-1}, \ldots, f_1))$ and S. Since f is similarity free, $\bar{g}_j = \bar{f}_w^{(0)}$. By the argument for the case when $f_k^{(0)}$ was chosen in step 3.1, `FactorsToRight` finds a decomposition consistent with $(f, (f_m, f_{m-1}, \ldots, f_1))$ and S. $\square$

In `FactorsToRight` we execute $t \leq \nu$ iterations of the main loop in step 3. In iteration i for $1 \leq i \leq t$, step 3.1 will require up to i transmutations of additive polynomials of exponents at most $\nu - i$. This requires $O(i(\mathbf{S}_F(p^{\nu-i}) + p^{3i}))$ field operations. Transforming the factors of this transmutation in step 3.3 using `TransformComposition` requires $O((\nu - i)^3 \log p)$ field operations. The total number of field operations required in iteration i is

$$\begin{aligned}&O(i\mathbf{S}_F(p^{\nu-i}) + ip^{3i} + (\nu - i)^3 \log p) \\ &= O(i\mathbf{S}_F(p^{\nu-i}) + ip^{3i}).\end{aligned}$$

The number of field operations required for all $t = O(\log n)$ iterations is therefore

$$\begin{aligned}
&\sum_{0\le i\le t} O(i\mathbf{S}_F(p^{\nu-i}) + ip^{3i}) \\
&= O(\nu\mathbf{S}_F(p^\nu) + \nu p^{3\nu}) \\
&= O(\mathbf{S}_F(n)\log n + n^3\log n).
\end{aligned}$$

We can now write a complete algorithm for the bidecomposition of similarity free additive polynomials.

`SimFreeBidecomp:` $\mathbb{A}_F \times \mathbb{N}^2 \to cAPDEC^F_*$

`Input:` - $f \in \mathbb{A}_F$, `similarity free of degree` $n = p^\nu$.

`Output:` - (p^ρ, p^σ), `an ordered factorisation of` n.

`1) Using CompleteDecomposition, attempt to find a decomposition` $(f, (f_m, f_{m-1}, \ldots, f_1)) \in cAPDEC^F_*$.

`2) For each subset` S `of` $\{1, \ldots, m\}$

`2.1) if` $\sum_{i\in S} \operatorname{expn} f_i = \sigma$, `find a decomposition` $(f, (g_m, g_{m-1}, \ldots, g_1))$ `consistent with` $(f, (f_m, f_{m-1}, \ldots, f_1))$ `and` S `using FactorsToRight. If such a decomposition is found, goto step 4.`

`3) There is no decomposition of` f `in` $cAPDEC^F_{(p^\rho,p^\sigma)}$, `quit.`

`4) Let` k `be such that` $g_m \circ g_{m-1} \circ \cdots \circ g_k$ `has exponent` ρ.

`5) Return` $(f, ((g_m \circ g_{m-1} \circ \cdots \circ g_k), (g_{k-1} \circ g_{k-2} \cdots \circ g_1)))$.

There are at most $2^\nu = O(n)$ subset S of $\{1, \ldots, m\}$ so the total number of field operations required is

$$O(\mathbf{S}_F(n)n\log n + n^4\log n).$$

We have shown the following theorem:

Theorem 5.19. *Let $f \in \mathbb{A}_F$ be similarity free of degree $n = p^\nu$. Let (p^ρ, p^σ) be an ordered factorisation of n. Using* `SimFreeBidecomp` *we can determine if there exists a decomposition of f in $APDEC^F_{(p^\rho,p^\sigma)}$, and if so find one, with $O(\mathbf{S}_F(n)n\log n + n^4\log n)$ field operations.*

5.9 Absolute Decompositions of Additive Polynomials

As noted in chapter 3, additive polynomials decompose into p-linear factors over their splitting fields. We will now show how to compute an arbitrary decomposition of an additive polynomial $f \in F[x]$ in an algebraic closure $\bar{F}$ of F (an absolute, complete decomposition).

Let $f \in \mathbb{A}_F$ have exponent ν, splitting field $K \subseteq \bar{F}$ and kernel V. We know any p-linear right factor $h = x^p - ax$ where $a \in K$ of f has a one dimensional kernel W which is a subspace of V. For any root $\alpha \neq 0$ of h, $a = \alpha^{p-1}$. It follows that the only possible p-linear right composition factors of f have $(p-1)^{\text{st}}$ powers of roots of f/x in K as the coefficients of their constant terms. Therefore $(x^p - ax) \mathbin{\phi} f$ if and only if $a \in K$ is a root of $(f/x) \circ x^{1/(p-1)}$. Assume F_i is a field (to be defined later) for $1 \leq i \leq \nu$ and that $F = F_\nu \subseteq F_{\nu-1} \subseteq F_{\nu-2} \subseteq \cdots \subseteq F_1 \subsetneq \bar{F}$.

`AbsAPDecomp:` $\mathbb{A}_{\bar{F}} \to cAPDEC_*^{\bar{F}}$

`Input :-` $f^{(i)} \in \mathbb{A}_{F_i}$ `monic of exponent` i, `for some` $i \in \mathbb{N}$.

`Output :- a complete decomposition of` f `in` $cAPDEC_*^{\bar{F}}$.

`If` $i = 1$

`then return` $f^{(1)} \in F_1[x]$.

`Otherwise`

1) `factor` $h^{(i)} = (f^{(i)}/x) \circ x^{\frac{1}{p-1}} \in F[x]$ `such that` $h^{(i)} = u_1^{e_1} u_2^{e_2} \cdots u_m^{e_m}$ `where` $u_j \in F[x]$ `are distinct, monic and irreducible and` $e_j \in \mathbb{N} \setminus \{0\}$ `for` $1 \leq j \leq m$.
2) `Let` $a = z \bmod u_1 \in F_{i-1} = F_i[z]/(u_1)$.
3) `Compute` $g^{(i)} = f^{(i)} \oint (x^p - ax) \in F_{i-1}[x]$.
4) `Recursively compute an absolute decomposition` $(g^{(i)}, (v_m, v_{m-1}, \ldots, v_2)) \in cAPDEC_*^{\bar{F}}$ `using AbsAPDecomp.`
5) `Return` $(f^{(i)}, (v_m, v_{m-1}, \ldots, v_2, u_1)) \in cAPDEC_*^{\bar{F}}$.

Each recursive stage i (starting with stage ν) requires the factoring of a polynomial of degree at most $(p^i - 1)/(p-1) \leq p^i$ in F_i. The degree of F_{i-1} over F_i is at most $(p^i - 1)/(p-1) \leq p^i$. It follows that the degree of F_i over $F = F_\nu$ is at most

$$\begin{aligned} \prod_{i<j\leq\nu} [F_{j-1} : F_j] &\leq \prod_{i<j\leq\nu} p^j \\ &\leq p^{\nu(\nu-i)}. \end{aligned}$$

Therefore, at recursive stage i, the number of field operations required is at most

$$\mathbf{S}_F(p^i)M(p^{\nu(\nu-i)})$$

and the total cost is

$$\sum_{0\le i\le \nu} \mathbf{S}_F(p^i)M(p^{\nu(\nu-i)}) \le M(p^{\nu^2})\mathbf{S}_F(p^\nu).$$

We have shown the following:

Theorem 5.20. *Given $f \in \mathbb{A}_F$ monic of degree $n = p^\nu$, we can find an absolute decomposition of f in $cAPDEC_*^{\bar{F}}$ in $O(M(p^{\nu^2})\mathbf{S}_F(p^\nu)) = n^{O(\log n)}$ field operations over F provided F supports a polynomial time factoring algorithm.*

Suppose F is finite. It is conjectured that an additive polynomial $f \in \mathbb{A}_F$ of degree $n = p^\nu$ can have a splitting field K of degree at most $n^{O(1)}$ over F, and quite possibly at most n. This would follow immediately from a (much stronger) unproven conjecture of Ore[1933b] that the degrees of all irreducible factors of f divide the degree t of the largest multiplicative factor of f. This would imply that $[K : F] = t$, and that the above algorithm for absolute decomposition would run in a polynomial number (in n) of field operations over F.

6 Rational Function Decomposition

Let $f \in F(x)$ be a rational function in x. A natural question to ask is if f can be represented as a composition of two other rational function $g, h \in F(x)$, so that $f = g \circ h$. This problem has polynomial decomposition as a small subcase. Mathematically, rational function decomposition has been examined since Ritt[1923]. The Generalised Schur Problem for rational functions involves the classification of so called "virtually one to one" rational functions and their decompositions. In general, rational function decomposition is far from completely understood. An in depth coverage and survey of the problem is presented in Fried[1974], where a generalisation of the tame case for polynomial decomposition in perfect fields is described (and is well beyond the scope of this thesis). In this chapter we present a definition of the rational function decomposition problem in a form similar to our presentation of the polynomial decomposition problem. We show that such decompositions can be normalised in a manner similar to polynomial decomposition and that the general problem is Cook reducible to the normal problem. We then give a computational solution to the normal decomposition problem for rational functions (which will require an exponential number of field operations in the input degree and a factorisation algorithm over F).

6.1 The Normalised Decomposition Problem

If $f \in F(x)$ then $f = f_N/f_D$ for some $f_N, f_D \in F[x]$ of degrees n_N and n_D respectively. We can assume that f_N and f_D are relatively prime and that f_D is monic. For any rational function f, there is a unique pair of polynomials $f_N, f_D \in F[x]$ with f_D monic and $\gcd(f_N, f_D) = 1$ such that $f = f_N/f_D$. With this in mind, define

$$\mathbb{U}_F = \{(f, (f_N, f_D)) \in F(x) \times F[x]^2 \mid f = f_N/f_D,\ \gcd(f_N, f_D) = 1, f_D \text{ monic}\}.$$

If $(f, (f_N, f_D)) \in \mathbb{U}_F$ and f_N is monic, we say f is monic. Also define $\deg f = n_N + n_D$ and $\Delta(f) = n_N - n_D$. The only automorphisms of the field $F(x)$ over F are the fractional linear transformations

$$x \mapsto \frac{t_1 x + t_2}{t_3 x + t_4},$$

where $t_1, t_2, t_3, t_4 \in F$ and $t_1 t_4 - t_2 t_3 \neq 0$. The inverse of the the above map is

$$x \mapsto \left(\frac{1}{t_1 t_4 - t_2 t_3}\right) \frac{t_4 x - t_2}{-t_3 x + t_1}.$$

Note that this group is isomorphic to $GL_2(F)$, the group of 2×2 non-singular matrices over F. Note also that if $f = f_N / f_D \in F(x)$, then

$$\frac{t_1 x + t_2}{t_3 x + t_4} \circ f = \frac{t_1 f_N + t_2 f_D}{t_3 f_N + t_4 f_D}.$$

Let $f, g, h \in F(x)$ with $f = g \circ h$, and let $t \in F(x)$ be a fractional linear transformation. We see that $f = (g \circ t^{-1}) \circ (t \circ h)$ is also a decomposition of f. Two decomposition $f = g \circ h$ and $f = g' \circ h'$ are said to be *linearly equivalent* if there exists a fractional linear transformation $t \in F(x)$ such that $g = g' \circ t^{-1}$ and $h = t \circ h'$. Let $(f, (f_N, f_D)) \in \mathbb{U}_F$ and $(r_N, r_D, s_N, s_D) \in \mathbb{N}^4$. Define

$$RATDEC^F_{(r_N, r_D, s_N, s_D)} = \begin{cases} (f, (g,\ h)) \in F(x) \times F(x)^2,\ f = g \circ h, \\ \qquad (g, (g_N, g_D)), (h, (h_N, h_D)) \in \mathbb{U}_F, \\ \qquad \deg g_N = r_N,\ \deg g_D = r_D, \\ \qquad \deg h_N = s_N,\ \deg h_D = s_D. \end{cases}$$

For any $f \in F(x)$ and $(r_N, r_D, s_N, s_D) \in \mathbb{N}^4$ there are potentially a large (possibly infinite, depending upon F) number of decompositions of f in $RATDEC^F_{(r_N, r_D, s_N, s_D)}$ (though up to linear equivalence we will see there are at most a linearly exponential number). The *rational function decomposition problem* is, given $f \in F(x)$ and $r_N, r_D, s_N, s_D \in \mathbb{N}$, to determine if there exist any decompositions of f in $RATDEC^F_{(r_N, r_D, s_N, s_D)}$, and, if so, to find one or all of them up to linear equivalence.

Let $(f, (f_N, f_D)), (g, (g_N, g_D)), (h, (h_N, h_D)) \in \mathbb{U}_F$. Assume $f_N, f_D, g_N, g_D, h_N, h_D \in F[x]$ have degrees $n_N, n_D, r_N, r_D, s_N, s_D$ respectively, and that they are of the form

$$\begin{aligned} f_N &= \sum_{0 \leq i \leq n_N} a_i x^i, \quad & f_D &= \sum_{0 \leq i \leq n_D} \bar{a}_i x^i, \\ g_N &= \sum_{0 \leq i \leq r_N} b_i x^i, \quad & g_D &= \sum_{0 \leq i \leq r_D} \bar{b}_i x^i, \\ h_N &= \sum_{0 \leq i \leq s_N} c_i x^i, \quad & h_D &= \sum_{0 \leq i \leq s_D} \bar{c}_i x^i. \end{aligned}$$

Let

$$A = \sum_{0 \le i \le r_N} b_i {h_N}^i {h_D}^{r_N - i} = {h_D}^{r_N}(g_N \circ h) \in F[x],$$
$$B = \sum_{0 \le j \le r_D} \bar{b}_j {h_N}^j {h_D}^{r_D - j} = {h_D}^{r_D}(g_D \circ h) \in F[x].$$

If $f = g \circ h$ then

$$f = \frac{A {h_D}^{-r_N}}{B {h_D}^{-r_D}} = \begin{cases} \dfrac{A}{B {h_D}^{r_N - r_D}} & \text{if } r_N > r_D \\ \dfrac{A {h_D}^{r_D - r_N}}{B} & \text{if } r_N \le r_D \end{cases}$$

Note that

$$\deg A = \begin{cases} r_N s_N & \text{if } s_N > s_D, \\ r_N s_D & \text{if } s_N < s_D. \end{cases}$$

If $s_N = s_D$ then cancellation can occur and the strongest statement that can be made is that $\deg A \le r_N s_D$. Similarly,

$$\deg B = \begin{cases} r_D s_N & \text{if } s_N > s_D, \\ r_D s_D & \text{if } s_N < s_D. \end{cases}$$

Once again, if $s_N = s_D$, cancellation can occur, and the most we can say is that $\deg B \le r_D s_D$.

Lemma 6.1. *A,B, and h_D (as defined above) are pairwise relatively prime.*

Proof. We first show $\gcd(A, B) = 1$. Suppose to the contrary that $\gcd(A, B) \neq 1$. Then A and B have a common root $\beta \in \bar{F}$ (where $\bar{F}$ is an algebraic closure of F), and

$$A(\beta) = \begin{cases} [{h_D}^{r_N} g_N(h_N/h_D)](\beta) & \text{if } h_D(\beta) \neq 0, \\ b_{r_N} {h_N}^{r_N}(\beta) & \text{if } h_D(\beta) = 0, \end{cases}$$
$$B(\beta) = \begin{cases} [{h_D}^{r_D} g_D(h_N/h_D)](\beta) & \text{if } h_D(\beta) \neq 0, \\ \bar{b}_{r_D} {h_N}^{r_D}(\beta) & \text{if } h_D(\beta) = 0. \end{cases}$$

If $h_D(\beta) \neq 0$, it follows that $g_N(h(\beta)) = g_D(h(\beta)) = 0$, a contradiction since g_N and g_D are relatively prime. If $h_D(\beta) = 0$, then $A(\beta) = b_{r_N} {h_N}^{r_D}(\beta) \neq 0$

(since $\gcd(h_N, h_D) = 1$), contrary to the assumptions. Thus $\gcd(A, B) = 1$. We now show that A and h_D are relatively prime. First,

$$\begin{aligned}
\gcd(A, h_D) &= \gcd(\sum_{0 \le i \le r_N} b_i {h_N}^i {h_D}^{r_N - i}, h_D) \\
&= \gcd(b_{r_N} {h_N}^{r_N} + h_D \sum_{0 \le i \le r_N} b_i {h_N}^i {h_D}^{r_N - i - 1}, h_D) \\
&= \gcd(b_{r_N} {h_N}^{r_N}, h_D) \\
&= 1 \qquad \text{since } \gcd(h_N, h_D) = 1.
\end{aligned}$$

Similarly,

$$\begin{aligned}
\gcd(B, h_D) &= \gcd(\sum_{0 \le j \le r_D} \bar{b}_j {h_N}^j {h_D}^{r_D - j}, h_D) \\
&= \gcd(\bar{b}_{r_D} {h_N}^{r_D} + h_D \sum_{0 \le j \le r_D} \bar{b}_j {h_N}^j {h_D}^{r_D - j - 1}, h_D) \\
&= \gcd(\bar{b}_{r_D} {h_N}^{r_D}, h_D) \\
&= 1 \qquad \text{since } \gcd(h_N, h_D) = 1.
\end{aligned}$$

□

This implies that $f = (A/B){h_D}^{r_D - r_N}$ is in "lowest terms". For f as above, we call (n_N, n_D) the *degree pair* of f.

Lemma 6.2. *Given* $(f, (f_N, f_D)), (g, (g_N, g_D)), (h, (h_N, h_D)) \in \mathbb{U}_F$ *with respective degree pairs* $(n_N, n_D), (r_N, r_D)$, *and* (s_N, s_D), *where* $\Delta(f), \Delta(h) > 0$ *and* $f = g \circ h$, *it follows that* $\Delta(g) > 0$, $r_N = n_N / s_N$ *and*

$$r_D = \frac{n_D s_N - n_N s_D}{s_N (s_N - s_D)}.$$

Proof. We know that $f = (A/B){h_D}^{r_D - r_N}$, where $A, B \in F[x]$ are as defined previously. Assume $r_N \le r_D$. We have seen that $(f, (A{h_D}^{r_D - r_N}, B)) \in \mathbb{U}_F$ and $n_N = r_N s_N + r_D s_D - r_N s_D > r_D s_N = n_D$. A simple rearrangement reveals that $r_N(s_N - s_D) > r_D(s_N - s_D)$ and since $s_N > s_D$, we find that $r_N > r_D$, a contradiction. It must then be true that $r_N > r_D$ and $(f, (A, B{h_D}^{r_N - r_D})) \in \mathbb{U}_F$. From the previous discussion on the degrees of A and B, we know that $n_N = r_N s_N$ and $n_D = r_D s_N + s_D(r_N - r_D)$. Solving for r_N and r_D in these

equations, we derive that $r_N = n_N/s_N$ and

$$\begin{aligned} r_D(s_N - s_D) &= n_D - s_D r_N \\ &= \frac{n_D s_N - n_N s_D}{s_N} \end{aligned}$$

and finally that

$$r_D = \frac{n_D s_N - n_N s_D}{s_N(s_N - s_D)}.$$

□

This implies that the degree pair of g is totally determined by the degree pairs of f and h. We will later see that in fact f and h uniquely determine g.

The set of degree pairs of f and it images under fractional linear transformations forms a highly structured set.

Lemma 6.3. *Let* $f \in F(x) \setminus F$,

$$T = \{t \circ f \mid t \in F(x) \text{ a fractional linear transformation}\}$$

and

$$D = \{(c,d) \in \mathbb{N}^2 \mid (c,d) \text{ a degree pair of some } g \in T\}.$$

Then D has exactly three elements, and these are of the form (a,b), (b,a) and (a,a), for some $a, b \in \mathbb{N}$ with $a > b$.

Proof. Assume $(f,(f_N,f_D)) \in \mathbb{U}_F$ and f has degree pair (n_N,n_D). As noted earlier, if $t = (t_1x+t_2)/(t_3x+t_4) \in F(x)$ is a fractional linear transformation then $t \circ f = (t_1f_N+t_2f_D)/(t_3f_N+t_4f_D)$. We examine three cases. If $n_N > n_D$, then for any fractional linear transformation $t \in F(x)$, observation reveals that $t \circ f$ has possible degree pairs (n_N,n_D), (n_D,n_N) and (n_N,n_N). Similarly, if $n_D > n_N$, $t \circ f$ has possible degree pairs (n_N,n_D), (n_D,n_N) and (n_D,n_D). If $f_N = f_D$, let a_N be the leading coefficient of f_N and δ the degree of $f_N - a_N f_D$. Then $t \circ f$ can have degree pairs (n_N,n_N), (δ,n_N), and (n_N,δ). Since the fractional linear transformations form a group under composition, these are the only degree pairs. □

This allows us to normalise the rational function decomposition problem and show a reduction from the general problem to the normal problem. For any $(f,(f_N,f_D)) \in \mathbb{U}_F$, let $a_N \in F$ be the leading coefficient of f_N and let

$\gamma \in F$ be the leading coefficient of $f_N - a_N f_D$. Also, let $\alpha = a_N - 1 \in F$. Define Λ_f, a fractional linear transformation, as follows:

$$\Lambda_f = \begin{cases} x/a_N & \text{if } \Delta(f) > 0, \\ \gamma \cdot \left(\dfrac{x-\alpha}{x-a_N} \right) & \text{if } \Delta(f) = 0, \\ a_N/x & \text{if } \Delta(f) < 0. \end{cases}$$

Λ_f is a fractional linear transformation. Observation reveals that $\Lambda_f \circ f$ is monic and $\Delta(\Lambda_f \circ f) > 0$. If $f = g \circ h$ for $g, h \in F(x)$, then

$$\Lambda_f \circ f = (\Lambda_f \circ g \circ \Lambda_h^{-1}) \circ (\Lambda_h \circ h).$$

Therefore, we can assume for any decomposition of f that f and h are monic and $\Delta(f)$ and $\Delta(h)$ are both positive. By lemma 6.2 we know $\Delta(g)$ is positive as well. Because $f_N = \sum_{0 \le i \le r_N} b_i {h_N}^i {h_D}^{r_N - i}$, $s_N > s_D$, and f_N is monic, we also see that $b_{r_N} = 1$ and g is monic as well. A further normalisation can be made by noting that

$$\begin{aligned} f &= g \circ h \\ &= g(x + h(0)) \circ (h - h(0)). \end{aligned}$$

Assume $\Delta(h)$ is positive. Then $h - h(0) = (h_N - h(0)h_D)/h_D$ has the same degree pair as h. If $\Delta(f)$ and $\Delta(g)$ are also positive, it follows that $g(x+h(0))$ has the same degree pair as g as well since r_N and r_D are completely determined by n_N, n_D, s_N, and s_D, so we can assume $h(0) = 0$ in any decomposition. We call a decomposition of a monic rational function f with $\Delta(f) > 0$ into two monic rational function $g, h \in F(x)$ such that $\Delta(g) > 0$, $\Delta(h) > 0$ and $h(0) = 0$ a *normal decomposition* of f. Let $n_N, n_D, r_N, r_D, s_N, s_D \in \mathbb{N}$ be such that $n_N = r_N s_N$ and $n_D = r_N s_D - r_D s_D + r_D s_N$. Define

$$NRATDEC^F_{(r_N, r_D, s_N, s_D)} = \left\{ \begin{array}{l} (f, (g, h)) \in F(x) \times F(x)^2 : \\ \quad f, g, h \text{ monic},\ h(0) = 0,\ f = g \circ h, \\ \quad (f, (f_N, f_D)), (g, (g_N, g_D)), (h, (h_N, h_D)) \in \mathbb{U}_F, \\ \quad \Delta(f), \Delta(g), \Delta(h) > 0, \\ \quad \deg g_N = r_N,\ \deg g_D = r_D, \\ \quad \deg h_N = s_N,\ \deg h_D = s_D. \end{array} \right\}$$

Given a monic $f \in F(x)$ with $\Delta(f) > 0$, and $(r_N, r_D, s_N, s_D) \in \mathbb{N}^4$ such that $n_N = r_N s_N$ and $n_D = r_N s_D - r_D s_D + r_D s_N$, the *normalised rational function decomposition problem* is to determine if there exists $(f, (g, h)) \in NRATDEC^F_{(r_N, r_D, s_N, s_D)}$ and if so to find some predetermined number of them.

Note that unlike the polynomial decomposition problem, the degrees of the numerators and denominators of f, g and h are not left constant by the normalisations. We will now examine the relationship between the normal problem and the general problem by showing a linear time (in the input degree) reduction from the general problem to the normal problem.

Assume $f \in F(x)$ and $r_N, r_D, s_N, s_D \in \mathbb{N}$ are given as in the general problem. Also assume $(f, (f_N, f_D)) \in \mathbb{U}_F$ and $\bar{f} = \Lambda_f \circ f$ has $(\bar{f}, (\bar{f}_N, \bar{f}_D)) \in \mathbb{U}_F$ and degree pair $(\bar{n}_N, \bar{n}_D)$. The easiest case occurs when $s_N > s_D$. For each decomposition $(f, (g, h)) \in RATDEC^F_{(r_N, r_D, s_N, s_D)}$ there is a decomposition $(\bar{f}, (\bar{g}, \bar{h})) \in NRATDEC^F_{(\bar{r}_N, \bar{r}_D, s_N, s_D)}$, where $\bar{r}_N$ and $\bar{r}_D$ are determined as in lemma 6.2. Conversely, from any $(\bar{f}, (\bar{g}, \bar{h})) \in NRATDEC^F_{(\bar{r}_N, \bar{r}_D, s_N, s_D)}$ we can find a decomposition $(f, (\Lambda_f^{-1} \circ \bar{g}, \bar{h})) \in RATDEC^F_{(r_N, r_D, s_N, s_D)}$.

If $s_N < s_D$ we have another easy case since $\Lambda_h \circ h$ has degree pair (s_D, s_N). For each decomposition $(f, (g, h)) \in RATDEC^F_{(r_N, r_D, s_N, s_D)}$ there is a decomposition

$$(\bar{f}, (\bar{g}, \bar{h})) \in NRATDEC^F_{(\bar{r}_N, \bar{r}_D, s_D, s_N)}$$

where once again, we compute $\bar{r}_N, \bar{r}_D$ as in lemma 6.2. From any $(\bar{f}, (\bar{g}, \bar{h})) \in NRATDEC^F_{(\bar{r}_N, \bar{r}_D, s_D, s_N)}$ we can find a decomposition $(f, (\Lambda_f^{-1} \circ \bar{g} \circ (1/x), (1/x) \circ \bar{h})) \in RATDEC^F_{(r_N, r_D, s_N, s_D)}$.

Finally, if $s_N = s_D$, we have a difficulty in that the problem can be normalised in a number of different ways. Let $\bar{s}_D \in \mathbb{N}$ with $\bar{s}_D < s_N$, and find $\bar{r}_N, \bar{r}_D \in \mathbb{N}$ as in lemma 6.2 (if such an integer solution exists). For each decomposition $(f, (g, h)) \in RATDEC^F_{(r_N, r_D, s_N, s_D)}$ there is a decomposition $(\Lambda_f \circ f, (\Lambda_f \circ g, h)) \in NRATDEC^F_{(r_N', r_D', s_N, s_D)}$ for some appropriately calculated $r_N', r_D' \in \mathbb{N}$ (as in lemma 6.2). By lemma 6.3 there exists a fractional linear transformation $t \in F(x)$ such that $\Delta(t \circ h) > 0$ and $t \circ h$ is monic and has degree pair $(s_N, \bar{s}_D)$ for some $\bar{s}_D < s_N$. Thus $(\Lambda_f \circ f, (\Lambda_f \circ g \circ t^{-1}, t \circ h)) \in NRATDEC^F_{(\bar{r}_N, \bar{r}_D, s_N, \bar{s}_D)}$ for appropriately determined $\bar{r}_N, \bar{r}_D \in \mathbb{N}$. For any $(\bar{f}, (\bar{g}, \bar{h})) \in NRATDEC^F_{(\bar{r}_N, \bar{r}_D, s_N, \bar{s}_D)}$ we can find a decomposition $(f, (\Lambda_f^{-1} \circ \bar{g} \circ [1/(x-1)], [(x+1)/x] \circ \bar{h})) \in RATDEC^F_{(r_N, r_D, s_N, s_D)}$

(the fractional linear transformation $t = (x+1)/x$ [whose inverse is $1/(x-1)$] is such that $t \circ \bar{h}$ has degree pair s_N, s_N). This requires the solution of at most $s_N < \deg f$ normal problems. We have shown the following:

Theorem 6.4. *Assume we have an algorithm such that, given a monic $\bar{f} \in F(x)$ of degree n with $\Delta(\bar{f}) > 0$, and $(\bar{r}_N, \bar{r}_D, \bar{s}_N, \bar{s}_D) \in \mathbb{N}^4$, we can determine if there exist any $(\bar{f}, (\bar{g}, \bar{h})) \in NRATDEC^F_{(r_N, r_D, s_N, s_D)}$, and if so, find some predetermined number of them, in $O(T(n))$ field operations. Then, given $f \in F(x)$ of degree n and $(r_N, r_D, s_N, s_D) \in \mathbb{N}^4$, we can determine if there exist any $(f, (g, h)) \in RATDEC^F_{(r_N, r_D, s_N, s_D)}$, and if so, find some predetermined number of them, in $O(s_N T(n)) = O(nT(n))$ field operations.*

This is equivalent to saying that the general rational function decomposition problem is Cook reducible to the normal rational function decomposition problem, where the oracle for the normal problem is consulted s_N times.

6.2 Decomposing Normalised Rational Functions

In this section we present a general computational solution for the rational function decomposition problem. Throughout this section, for any $f \in F[x]$ of degree n and any $i \in \mathbb{N}$ such that $0 \leq i \leq n$, we let $\text{coeff}(f, i) \in F$ be the coefficient of x^i in f. We begin by showing a preliminary lemma.

Lemma 6.5. *Given $r \in \mathbb{N}$, $u \in F[x]$ monic of degree n, and $h \in F(x)$ monic with $h(0) = 0$, $(h, (h_N, h_D)) \in \mathbb{U}_F$ and $\Delta(h) > 0$, we can determine if there exists a monic $v \in F[x]$ of degree r such that $u = v(h){h_D}^r$ in $O(n \log n M(n))$ field operations.*

Proof. Assume h_N, h_D have degree s_N, s_D respectively. It follows that if v exists, and is of the form

$$v = \sum_{0 \leq i \leq r} b_i x^i$$

with $b_i \in F$ for $0 \leq i \leq r$ then

$$u = \sum_{0 \leq i \leq r} b_i {h_N}^i {h_D}^{r-i}.$$

Let $d = \max\{j : x^j \mid h_N\} \geq 1$. We see that for $\ell \in \mathbb{N}$,

$$\begin{aligned}\operatorname{coeff}(u, \ell d) &= \operatorname{coeff}(\sum_{0 \leq i \leq r} b_i {h_N}^i {h_D}^{r-i}, \ell d) \\ &= \operatorname{coeff}(\sum_{0 \leq i \leq \ell} b_i {h_N}^i {h_D}^{r-i}, \ell d) \\ &= b_\ell \operatorname{coeff}(h_N, d)^\ell \operatorname{coeff}(h_D, 0)^{r-\ell} + \operatorname{coeff}(\sum_{0 \leq i < \ell} b_i {h_N}^i {h_D}^{r-i}, \ell d).\end{aligned}$$

Since $\operatorname{coeff}(h_N, d) \neq 0$ and $\operatorname{coeff}(h_D, 0) \neq 0$, we know

$$b_\ell = \frac{\operatorname{coeff}(u, \ell d) - \operatorname{coeff}(\sum_{0 \leq i < \ell} b_i {h_N}^i {h_D}^{r-i}, \ell d)}{\operatorname{coeff}(h_N, d)^\ell \operatorname{coeff}(h_D, 0)^{r-\ell}}.$$

Using this recurrence we can compute the coefficients $b_0, b_1, \ldots, b_r \in F$ in order. Because the system is over constrained, the computed coefficients may not lead to a decomposition. Thus we must check if in fact $u = v(g){h_D}^r$. The cost of this computation is dominated by the cost of computing ${h_N}^i {h_D}^{r-i}$ for $0 \leq i \leq r$, which can be done with $O(n \log n M(n))$ field operations over F. □

The previous lemma allows us to perform "right division" in the ring of normal rational functions under composition.

Lemma 6.6. *Given $f, h \in F(x)$ monic with $h(0) = 0$ and $\Delta(f), \Delta(h) > 0$, we can determine if there exists a monic $g \in F(x)$ (with $\Delta(g) > 0$) such that $f = g \circ h$, and if so compute it, with $O(n \log n M(n))$ field operations.*

Proof. Assume $(f, (f_N, f_D)), (h, (h_N, h_D)) \in \mathbb{U}_F$. We want to find $(g, (g_N, g_N)) \in \mathbb{U}_F$ such that $f = g \circ h$. We know $f_N = (g_N \circ h){h_D}^{r_N}$ and using lemma 6.5 we can compute $g_N \in F[x]$ if it exists. We also know that $f_D / {h_D}^{r_N - r_D} = g_D(h){h_D}^{r_D}$, and so we can compute $g_D \in F[x]$ if it exists. The total number of field operations required is $O(n \log n M(n))$. □

We can now give an algorithm for the normal rational function decomposition problem. It will require an exponential number of field operations.

NormRatDec: $F(x) \times \mathbb{N}^4 \to \mathbf{P}(RATDEC^F)$
Input: - $f \in F(x)$ with $\Delta(f) > 0$ and $(f,(f_N,f_D)) \in \mathbb{U}_F$ where f_N and f_D have degrees n_N and n_D respectively,
- $r_N, r_D, s_N, s_D \in \mathbb{N}$ such that $n_N = r_N s_N$ and $n_D = r_N s_D - r_D s_D + r_D s_N$.
Output: - the set of all decompositions of f in $RATDEC^F_{(r_N,r_D,s_N,s_D)}$.
1) Let $T := \emptyset$.
2) For each monic $h_D \in F[x]$ of degree s_D such that ${h_D}^{r_N - r_D} | f_D$, and $h_D(0) \neq 0$, do
2.1) Let $B := f_D / {h_D}^{r_N - r_D}$.
2.2) Let $\bar{b}_0 := f_D(0)/(h_D(0))^{r_N}$.
2.3) For each factor h_N of $B - \bar{b}_0 {h_D}^{r_D}$ of degree s_N,
2.3.1) Let $h := h_N / h_D$.
2.3.2) Attempt to compute $g \in F(x)$ such that $f = g \circ h$ using lemma 6.6. If such a g exists for the chosen h, add $(f,(g,h))$ to T.
3) Return T.

We know that in any decomposition ${h_D}^{r_N - r_D} | f_D$, so in step 2 we generate all potential candidates for h_D. In step 2.2, since $f_D(0) = {h_D}^{r_N - r_D}(0) \bar{b}_0 {h_D}^{r_D}(0) = \bar{b}_0 {h_D}^{r_N}$, we can compute $\bar{b}_0 = f_D(0)/{h_D}^{r_N}(0)$. We use the identity

$$\begin{aligned} B - \bar{b}_0 {h_D}^{r_D} &= \sum_{1 \le j \le r_D} \bar{b}_j {h_N}^j {h_D}^{r_D - j} \\ &= h_N \sum_{1 \le j \le r_D} \bar{b}_j {h_N}^{j-1} {h_D}^{r_D - j} \end{aligned}$$

to get all candidates for h_N, namely all degree r_N factors of $B - \bar{b}_0 {h_D}^{r_D}$. In step 2.3.1 we simply check whether the chosen $h = h_N / h_D$ leads to a decomposition. The algorithm certainly requires an exponential number of field operations in the input size because for any $f \in F[x]$ of degree n, there are potentially 2^n factors of f. Therefore, the cost of the algorithm is dominated by the cost of computing step 2.3.2 as many as $(2^n)^2$ times, each time requiring $O(n \log n M(n))$ field operations. We have shown the following theorem.

Theorem 6.7. *The normal rational function decomposition problem can be solved with* $O(2^{2n} n \log n M(n))$ *field operations.*

Using theorem 6.4 we get the following corollary for the general case:

Corollary 6.8. *The rational function decomposition problem can be solved with* $O(2^{2n} n^2 \log n M(n))$ *field operations.*

7 Conclusion.

We formally presented the decomposition problem for polynomials (both univariate and multivariate) in a number of formulations and showed their equivalence. We then presented a survey of the known algorithms for the decomposition problem in light of this consistent mathematical basis. A reduction is shown from the general (multiple composition factor) decomposition problem to the bidecomposition problem for "nice" classes of polynomials. In the wild case we exhibited super-polynomial lower bound on the number of decompositions of a polynomial which can exist by examining the additive polynomials, for which all decompositions are wild. We dealt with the additive case algorithmically as well, demonstrating a polynomial time algorithm for generating a complete decomposition (and hence determining indecomposability). It is shown that the decomposition problem for additive polynomials can be solved in quasi-polynomial time. We also showed that the general decomposition problem for completely reducible additive polynomials and the bidecomposition problem for similarity free additive polynomials can be solved in polynomial time. The rational function decomposition problem is also defined and it is shown how to normalise this problem appropriately, such that the general problem is reducible to the normal one. We then showed how to solve the normalised rational function decomposition problem in a polynomial number of field operations.

Many open questions remain in the wild case for polynomial decomposition. The additive polynomials represent a small but important subcase of these polynomials and yet even here no polynomial time algorithm is known for even the bidecomposition problem. It is strongly suspected by the author that such an algorithm exists. Interesting questions also remain concerning the computation of absolute decompositions. It may be true that even over "well-behaved" fields such as finite fields that the coefficients of an absolute decomposition generate an extension of exponential degree over the ground

field. And of course, the main open question is still the existence of a polynomial time algorithm for the rational polynomial decomposition problem in the wild case. The rational function decomposition problem is only dealt with briefly here and many interesting questions remain unsolved. Most of these problems are extremely difficult, and the mathematical theory is very incomplete. Polynomial time algorithms, even for special cases, would be of great interest.

References

V.S. Alagar and M. Thanh, "Fast Polynomial Decomposition Algorithms," *Proceedings of EUROCAL 1985, Lecture Notes in Computer Science* **204**, Springer Verlag, Heidelberg, 1985, pp. 150–153.

D.R. Barton and R. Zippel, "Polynomial Decomposition Algorithms," *Journal of Symbolic Computation, Vol. 1*, 1985, pp. 159–168.

R.P. Brent and H.T. Kung, "Fast Algorithms for Composition and Reversion of Multivariate Power Series," *Proceedings of the Conference on Theoretical Computer Science*, University of Waterloo, Waterloo, Ontario, Canada, 1977, pp. 149–158.

R.P. Brent and H.T. Kung, "Fast Algorithms for Manipulating Formal Power Series," *Journal of the ACM, Vol. 25, No. 4*, 1978, pp. 581–595.

D.G. Cantor and E. Kaltofen,"Fast Multiplication of Polynomials over Arbitrary Rings", Preliminary Report, 1987.

T.H.M. Crampton and G. Whaples, "Additive Polynomials II," *Transactions of the AMS, Vol. 78*, 1955, pp. 239–252.

M. Dickerson, "Polynomial Decomposition Algorithms for Multivariate Polynomials", *Department of Computer Science, Cornell University, Technical Report 87-826*, 1987.

F. Dorey and G. Whaples, "Prime and Composite Polynomials," Journal of Algebra, Vol. 28, 1974, pp. 88–101.

H.T. Engstrom, "Polynomial Substitutions," American Journal of Mathematics, Vol. 63, 1941, pp. 249–255.

A. Evyatar and D.B. Scott, "On Polynomials in a Polynomial," Bulletin of the London Mathematical Society, Vol. 4, 1972, pp. 176–178.

M.D. Fried and R.E. MacRae [1969a], "On the Invariance of Chains of fields," *Illinois Journal of Mathematics, Vol. 13*, 1969, pp. 165–171.

M.D. Fried and R.E. MacRae [1969b], "On Curves with Separated Variables," Annals of Mathematics, Vol. 180, 1969, pp. 220–226.

M.D. Fried, "Arithmetical Properties of Function Fields (II). The Generalized Schur Problem," *Acta Arithmetica, Vol. 25*, 1974, pp. 225–258.

J. von zur Gathen[1986], "Parallel Arithmetic Computations: a survey." Proceedings of the 12^{th} International Symposium on the Mathematical Foundations of Computer Science, Bratislava, Springer Lecture Notes in Computer Science 233, 1986, 93-112.

J. von zur Gathen[1987], "Functional Decomposition of Polynomials: the Tame Case," Technical Report, Sondersforschungsbereich 124, Universität des Saarlandes, Saarbrücken, August 1987.

J. von zur Gathen[1988], "Functional Decomposition of Polynomials: the wild Case," Manuscript in preparation, June 1988.

J. von zur Gathen, D. Kozen, S. Landau, "Functional Decompositions of Polynomials," Procedings of the 28^{th} annual IEEE Symposium on the Foundations of Computer Science, Los Angeles CA, 1987, pp. 127-131.

G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers.* Clarendon Press, Oxford, 1962.

D. Kozen and S. Landau, "Polynomial Decomposition Algorithms," *Department of Computer Science, Cornell University, Technical Report 86-773*, 1986. (to appear in the Journal of Symbolic Computation).

S. Landau and G.L. Miller, "Solvability by Radicals is in Polynomial Time," *Journal of Computer Systems Science, Vol. 30*, 1985, pp. 179–208.

H. Levi, "Composite Polynomials with Coefficients in an Arbitrary Field of Characteristic Zero," *American Journal of Mathematics, Vol. 64*, 1942, pp. 389–400.

R. Lidl and H. Niederreiter, "Introduction to Finite Fields and Their Applications," Cambridge University Press, Cambridge, 1986.

J.D. Lipson, "Newton's Method: A Great Algebraic Algorithm," *Proceedings of ACM Symposium on Symbolic and Algebraic Computation*, 1976, pp. 260–270.

O. Ore [1933a], "Theory of Non-Commutative Polynomials," *Annals of Mathematics, Vol. 34, No. 2*, 1933, pp. 480–508.

O. Ore [1933b], "On a Special Class of Polynomials," *Transactions of the AMS, Vol. 35*, 1933, pp. 559–584.

O. Ore, "Contributions to the Theory of Finite Fields," *Transactions of the AMS, Vol. 36*, 1934, pp. 243–274.

J.F. Ritt[1922], "Prime and Composite Polynomials," *Transactions of the AMS, Vol. 23*, 1922, pp. 51–66.

J.F. Ritt[1923], "Permutable Rational Functions," *Transactions of the AMS, Vol. 25*, 1923, pp. 399-448.

J. B. Rosser and Lowell Schoenfeld, "Approximate Formulas For Some Functions Of Prime Numbers", *Illinois Journal of Mathematics, Vol. 6*, 1962, pp. 64-94.

Schönhage, Schnelle Multipikation von Polynomen über Körpern der Charakteristik 2. Acta Informatica 7 (1977), 395-398.

J.T. Schwartz, "Fast Probilistic Algorithms for the Verification of Polynomial Identities", *Journal of the ACM, Vol. 27, No. 4*, October 1980, pp. 701-717.

B.L. van der Waerden, "Modern Algebra, Vol. 1," Fredrick Unger Publishing Co., New York, 1949.

G. Whaples, "Additive Polynomials," *Duke Mathematical Journal, Vol. 21*, 1954, pp. 55–63.